Informe por política de Gestión y Desempeño

Política de Seguridad Digital

BOGOTÁ, 2024

Contenido

Presentación

El **Modelo Integrado de Planeación y Gestión (MIPG)** establece que el seguimiento y evaluación de sus políticas se realiza a través del Formulario Único de Reporte de Avance de la Gestión (FURAG). Este instrumento permite medir el desempeño institucional mediante **el Índice de Desempeño Institucional (IDI)** y otros índices asociados a sus políticas y dimensiones. Desde la actualización del MIPG en 2017, el Departamento Administrativo de la Función Pública (DAFP) ha liderado mediciones anuales del desempeño, realizando ajustes en el FURAG para incorporar nuevas políticas como "Compras y contratación pública" y "Gestión de la información estadística", lo que generó una nueva línea base en 2022 que impide comparaciones directas con años anteriores.

Para la vigencia 2023, el DAFP estableció los lineamientos mediante la Circular Externa 100-006 de 2024, y el registro de información en el FURAG se realizó entre abril y mayo. Los resultados del IDI fueron publicados en julio, proporcionando datos clave sobre el avance en la implementación de las políticas del MIPG.

Este informe corresponde específicamente a la **Política de Gestión y Desempeño de Seguridad Digital**, analizando los resultados de 2023 frente a los de 2022. En este documento se busca identificar fortalezas, necesidades de mejora y oportunidades para definir acciones que contribuyan al fortalecimiento institucional, tanto en la entidad líder distrital como en las demás entidades distritales.

Alcance de la medición de la Política de Seguridad Digital

El alcance del presente documento, demuestra el estado en la implementación de la política relativa a la seguridad digital en el distrito, en el marco de la implementación del MIPG, destacando el cumplimiento de las entidades, y los retos y oportunidades de mejora, para focalizar las acciones en posteriores vigencias.

Resultados Comparativos de las Políticas de Gestión y Desempeño

De conformidad con los resultados de la Medición del Desempeño Institucional, el promedio distrital de los índices asociados a las políticas de gestión y desempeño se ve representado en la gráfica No. 1.

En esta gráfica se evidencia que se han medido 17 políticas de Gestión y desempeño y de estas, el 76,4% presentan resultados superiores al promedio del IDI nacional, lo que puede deducir que estas políticas representan elementos de referencia para las entidades públicas del orden nacional y territorial. Por otra parte, se evidencia que las políticas de racionalización de trámites, gestión documental y gobierno digital requieren del diseño de acciones que aporten a su fortalecimiento, siendo la política de Gestión documental un punto de atención por la disminución de su puntaje en 10,9 puntos con respecto al año anterior

Gráfica No. 1. IDI promedio distrital para las políticas de Gestión y desempeño evaluadas.

Fuente: Informe por política de Gestión y Desempeño, Seguridad Digital

En relación con la política de seguridad digital, se avanzó en el compendio de la implementación en las entidades distritales, en u promedio de 7.2%; resaltando el compromiso de las diferentes entidades en avances del tipo normativo, documental y de implementación de controles que no implican grandes inversiones en términos presupuestales.

Resultados Política de Seguridad Digital

La Política de Seguridad Digital Mide la capacidad de la entidad pública de identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en las actividades socioeconómicas de la entidad en un entorno digital y en un marco de cooperación, colaboración y asistencia, con el fin de contribuir al crecimiento de la economía digital nacional. Esta se encuentra bajo el liderazgo de la Secretaría General de la Alcaldía Mayor de Bogotá, en Cabeza de la Oficina Consejeria Distrital de TIC

A continuación, se presenta el análisis del índice de la política, estableciendo un comparativo con el promedio territorial. Estos índices por política buscan asociar los logros por política con el avance en el índice.

El promedio distrital 2023 para esta política es 82,6 puntos, frente a un promedio de la medición territorial (alcaldía y gobernaciones) de 39,0 puntos. La brecha de 43,6 puntos con respecto los resultados en territorio denotan que el Distrito Capital es un referente para la aplicación de esta política a nivel territorial.

Los resultados por promedio de avance en la implementación de la política de seguridad digital, agrupados y organizados por los resultados por sectores se muestra en la siguiente imagen:

Imagen 1. Mapa de calor por Sectores

Fuente: Informe por política de Gestión y Desempeño, Seguridad Digital

Esta política obtuvo la quinceava puntuación a nivel distrital, donde ninguno de los sectores administrativos distritales presentó valores para esta política que superaran los resultados del IDI promedio distrital 2023 (89,6). Estos resultados deben entenderse bajo un contexto de implementación y mejora continua en la cual se encuentran las entidades distritales que permita la creación de capacidades para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades.

Aspectos relevantes de la política como, la gestión de vulnerabilidades, la gestión de incidentes y la gestión de la continuidad del negocio y las operaciones; son recurrentes por mejorar en la mayoría de las entidades distritales.

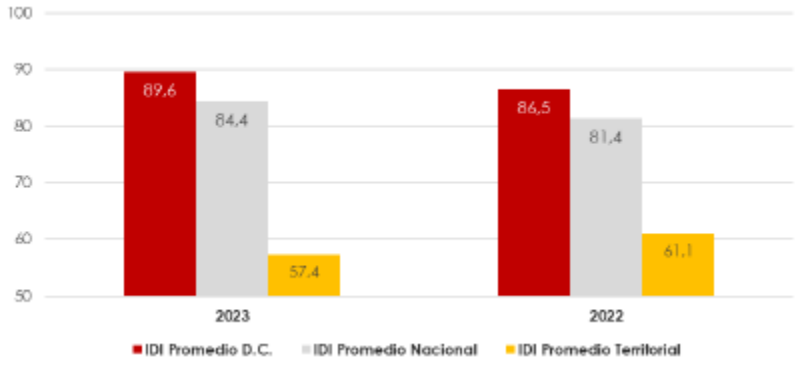
Lo anterior, por el fuerte énfasis de la política en una adecuada gestión de riesgos y su relación directa con el CONPES 3854, política nacional de seguridad digital.

Resultados Promedio Distrito Capital

A continuación, se presenta el Índice de Desempeño Institucional promedio del Distrito Capital. Esta medición se calcula a partir del promedio de los resultados obtenidos por las 50 entidades que hacen parte del grupo para Distrito Capital, incluyendo la medición de la Alcaldía mayor, como integrante de este segmento.

En el caso del promedio del Índice de Desempeño Institucional – IDI de las entidades del Distrito Capital fue de 89,6 puntos para el 2023, que aumenta en 3,1 puntos la medición del año 2022 y sobrepasan en 5,2 puntos el IDI promedio Nacional y en 32,2 puntos el IDI promedio territorial, cuyo resultado para el 2023 alcanzó los 57,4 puntos, debido a la inclusión de entidades en el ámbito de aplicación para esta vigencia.

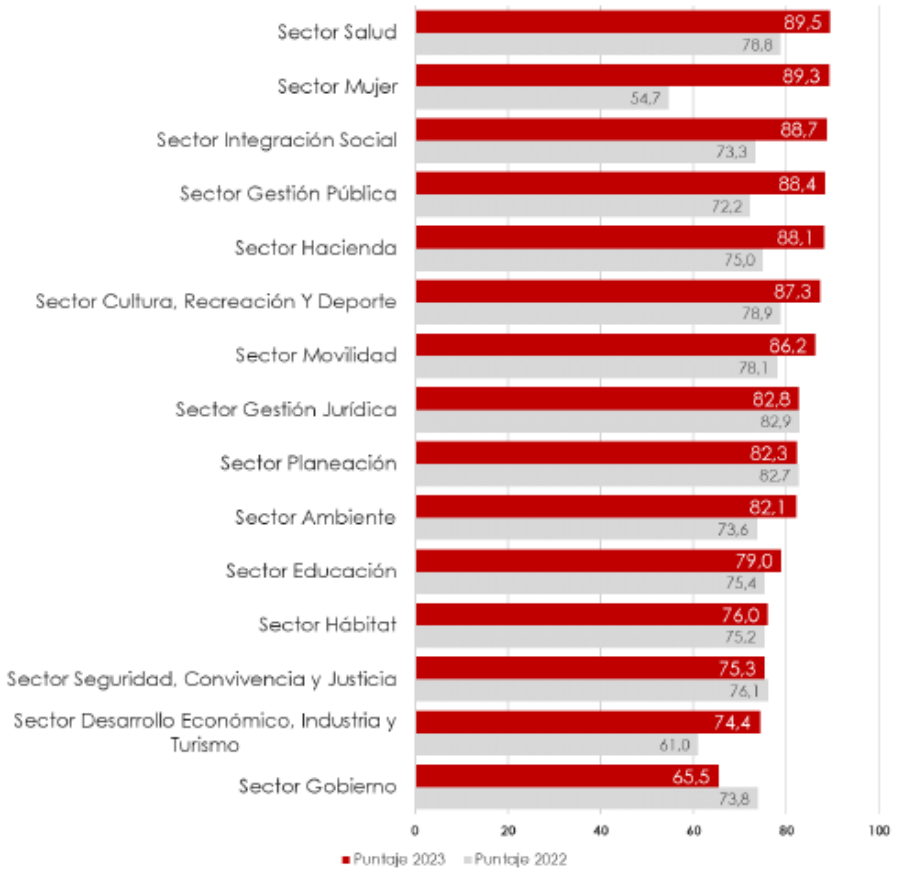
Gráfica No. 2. IDI Promedio Distrital comparado con el promedio nacional y territorial. 2022 y 2023



Fuente: Informe por política de Gestión y Desempeño, Seguridad Digital

La desagregación del Índice de esta política para las vigencias 2022 y 2023, asociado a los sectores administrativos presenta los siguientes resultados:

Gráfica No. 3. Puntaje agregado por sector administrativo. Seguridad Digital 2023



Fuente: Informe por política de Gestión y Desempeño, Seguridad Digital

Esta política obtuvo en ocho (8) de sus puntajes promedio por sector para la vigencia 2023, valores por encima del promedio distrital 2023 para esta política (82.6), donde el 73,3% de los sectores mejoraron los resultados alcanzados en la vigencia 2022.

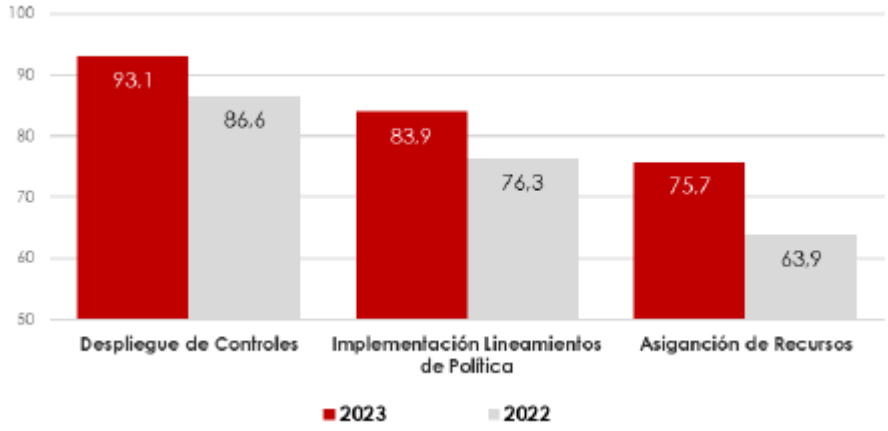
Análisis de los Subíndices de la Política

Esta política está compuesta bajo tres componentes o subíndices a saber:

- **Asignación de Recursos:** Relacionado con la asignación de recursos para el despliegue de la Política de Seguridad Digital, para proteger la información bajo su custodia.

- **Implementación Lineamientos de Política:** Se relaciona con la implementación de los lineamientos de política pública en materia de seguridad digital
- **Despliegue de Controles:** El cual se relaciona con establecer e implementar puntos de control básicos para mitigar los riesgos de seguridad digital

Gráfica No. 4. Subíndices de la Política de Seguridad Digital 2023



Fuente: Informe por política de Gestión y Desempeño, Seguridad Digital

Análisis del habilitador transversal de la política de gobierno digital

El Modelo de Seguridad y Privacidad de la Información – MSPI, establece los lineamientos a las entidades públicas en la implementación y adopción de buenas prácticas en protección de la información, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.

La Oficina Consejeria Distrital de TIC realiza el seguimiento y acompañamiento a la implementación de este modelo en las entidades del distrito capital. Tomando como base los resultados de los instrumentos de evaluación del MSPI aplicados en las entidades distritales se obtuvo la medición y análisis en la vigencia del 2023 de

61 entidades distritales que aplicaron dicho instrumento, presentando los siguientes resultados de la implementación del MSPI:

Gráfica No. 5. Nivel de madurez en MSPI de las entidades en 2023

Fuente: Elaboración propia Secretaria General Alcaldía Mayor de Bogotá

De la medición de la implementación del MSPI en la gestión de controles se identificó un promedio general de avance del 70% de las sesenta y uno (61)

Conclusiones

Aunque en 2023 las entidades distritales mejoraron su desempeño promedio en la Política de Seguridad Digital en comparación con el año anterior, existen grandes oportunidades de avanzar en la implementación de esta política en el Distrito, especialmente en lo que respecta:

- Implementación de controles tecnológicos y administrativos. Las entidades deben de avanzar en la definición e implementación de procesos orientados al monitoreo y gestión de riesgos y de vulnerabilidades, identificando superficies de ataque y gestionando adecuadamente su incidencia en los procesos misionales y de soporte.

- Definición de proyectos específicos en sus planes de estratégicos de tecnologías de información, que denoten gestión de vulnerabilidades, gestión de incidentes y gestión de la continuidad.
- Diseñar, definir y probar los planes de recuperación ante desastres de la plataforma tecnológica, en consideración al análisis de su procesos de soporte tecnológicos y alineados con la visión de transformación digital definida.
- Diseñar definir y probar sus planes de continuidad del negocio, en colaboración estrecha con la alta dirección, definiendo de manera consistentes los escenarios y riesgos de posibles afectaciones y contemplando procesos transversales y de negocio, no sólo sus habilitadores de TI.
- Identificar y realizar una adecuada valoración del riesgo de sus infraestructuras criticas cibernéticas, incluyendo tecnologías de operación (OT - IoT), si las poseen; y sus tradicionales tecnologías de TI.
- Incluir las evaluaciones de impacto a la privacidad de la información, en su gestión cíclica de riesgos y en la etapa previa a la salida a producción de nuevos sistemas, aplicativos o plataformas, que traten o recolecten datos personales.
- Definir superficies de ataque consistentes con la acción institucional y el apetito de riesgo aceptado por la entidad, involucrando nuevos vectores, como los presentados por el uso de la IA, en diferentes procesos institucionales.
- Reportar de manera eficiente sus incidentes de seguridad digital, al CSIRT DC y a las demás entidades con competencia en la materia, para ejercer una adecuada contención, mitigación y solución a este tipo de incidentes.