

INFORME EJECUTIVO DE POLÍTICA DE GESTIÓN Y DESEMPEÑO 2024

Política de Seguridad Digital



SECRETARÍA
GENERAL





Información general

Política: SEGURIDAD DIGITAL

Líder de política: Secretaría general – Oficina Consejería Distrital de Tecnologías de la Información y las Comunicaciones

Equipo técnico: Frederick Sánchez Neira

Correo institucional para envío y consultas: fsanchez@alcaldiabogota.gov.co

Fecha: Noviembre, 2025



1. Introducción

El presente informe analiza los resultados de la Política de Gestión y Desempeño de Seguridad Digital, a partir de la medición del Índice de Desempeño Institucional (IDI) 2024, realizada por el Departamento Administrativo de la Función Pública (DAFP), en el marco del Modelo Integrado de Planeación y Gestión (MIPG).

Su propósito es consolidar, interpretar y poner en contexto los principales resultados, hallazgos y brechas identificadas, así como formular recomendaciones técnicas y líneas de acción orientadas a fortalecer la implementación de la política en las entidades del Distrito Capital, en coherencia con los principios de planeación estratégica, gestión por resultados, seguimiento institucional y mejora continua de la gestión pública.

Para la información de la vigencia 2024, los lineamientos técnicos y metodológicos fueron definidos por el DAFP en la Circular Externa 100-003 de 2025, y el registro por medio del Formulario Único de Reporte de Avance de la Gestión – FURAG-, se llevó a cabo en los meses de marzo y abril.

En este sentido, este documento se constituye en una herramienta de apoyo para la toma de decisiones por parte de las directivas, al presentar de forma ejecutiva los principales resultados de la medición, desarrollar ejercicios de contrastación interanual, y proponer aproximaciones analíticas que permiten explicar el comportamiento de la política y de los indicadores que la componen, considerando tanto factores institucionales como elementos transversales del MIPG. Asimismo, busca fortalecer la capacidad de las entidades distritales para interpretar adecuadamente los resultados del IDI, priorizar acciones de mejora y alinear sus procesos de planeación, seguimiento y evaluación con los estándares definidos.

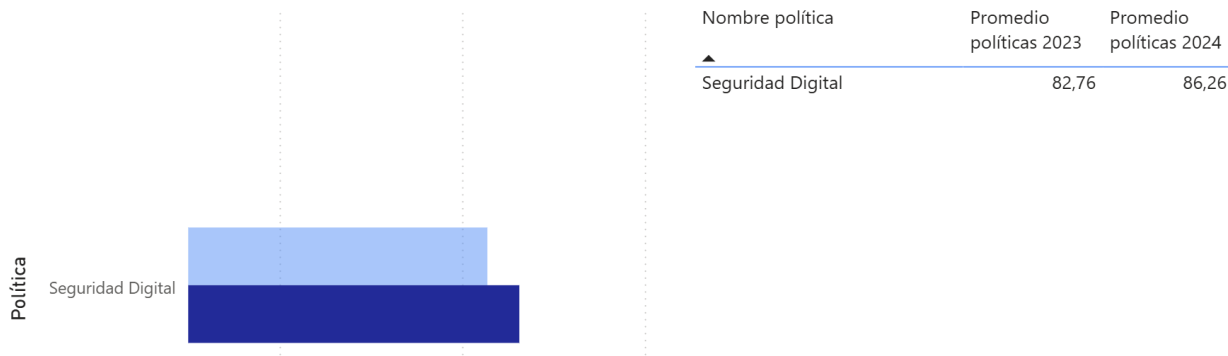
El documento integra el análisis comparativo de los resultados obtenidos, identifica oportunidades de mejora en la gestión de la Seguridad Digital y propone acciones estratégicas para potenciar la madurez digital, la protección de la información y la resiliencia tecnológica del Distrito, en coherencia con los principios de Gobierno Digital, ciberseguridad y sostenibilidad institucional.



2. Desempeño de la política en el IDI 2024

En la medición del Índice de Desempeño Institucional (IDI) 2024, la política de seguridad digital alcanzó un promedio de 86,26 puntos, lo que representa un incremento frente a la vigencia anterior. El resultado refleja como fortalezas principales el despliegue de controles y la implementación de lineamientos de política, evidenciando la necesidad de asignar mayores recursos para consolidar los avances en la siguiente medición. (Ver gráfica 1)

Gráfica 1. Puntaje política de Seguridad Digital

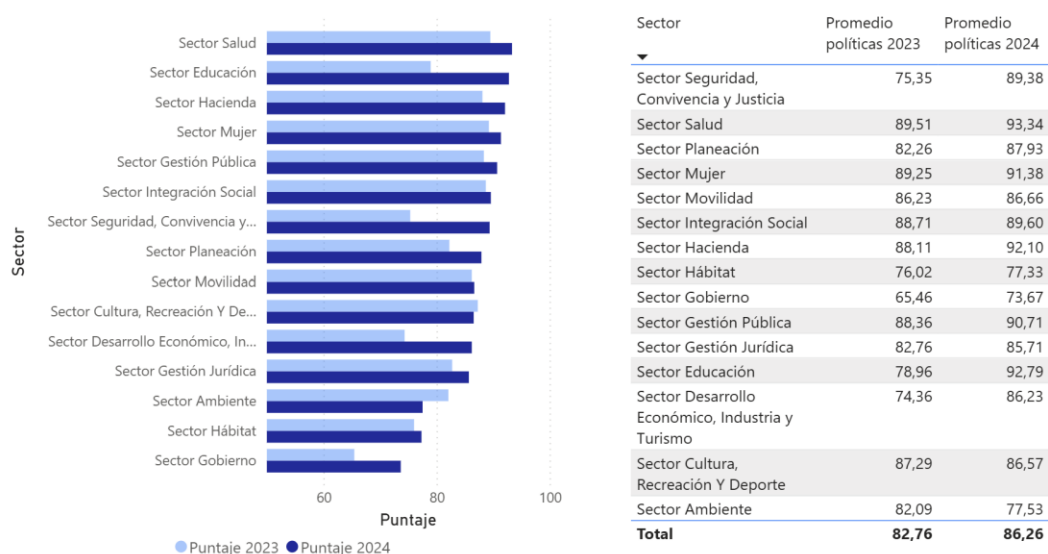


Fuente: Visor resultados IDI – Secretaría General

Ahora, desagregado por sectores, se encuentra que el sector con puntaje más alto es el sector seguridad, convivencia y justicia, obteniendo 89.38 puntos, aumentando con relación a la medición anterior. Igualmente, se evidencia que la variación promedio del año 2024 al 2023 es de 3.50 puntos, reflejando una significativa mejoría relativa (Ver gráfica 2)



Gráfica 2. Ranking por sector Distrital



Fuente: Visor resultados IDI – Secretaría General

Por otra parte, es importante destacar que esta política se compone de subíndices, que corresponden a los elementos estructurales que la conforman y que se visualizan en la gráfica 3.

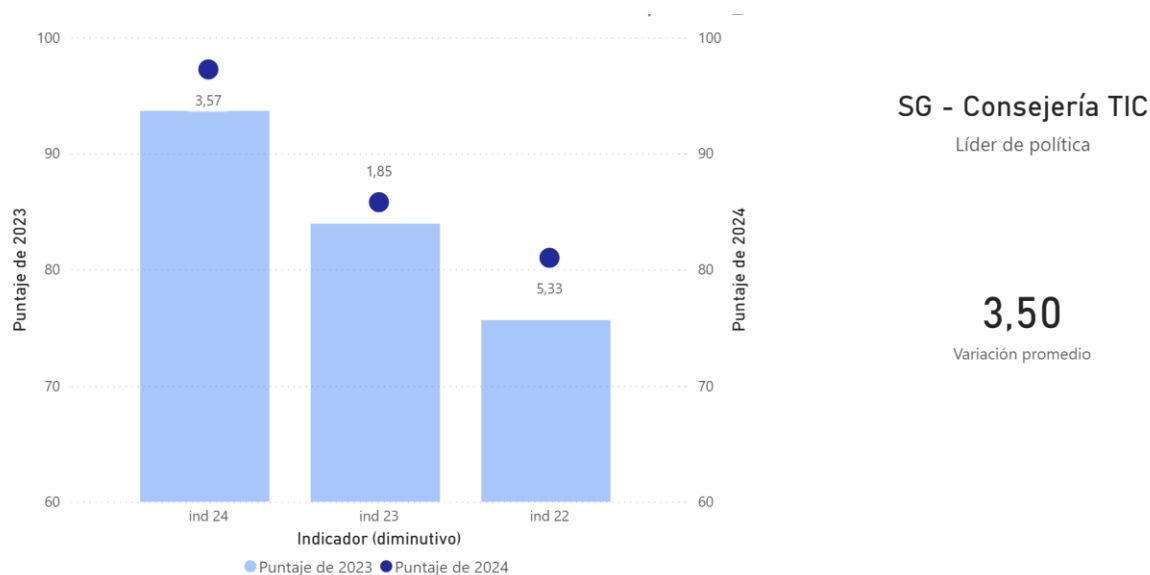
El primer subíndice corresponde a Despliegue de controles (Ind. 24) que registra un aumento de 3.57 puntos, respecto de la vigencia 2023. Esto se debe a que la gran mayoría de entidades documentó e implementó procedimientos para copias de respaldo y de restauración y las almacenó en un lugar aislado, en un segmento diferente de red a la de servidores y equipos, contó con equipos de seguridad perimetral para su infraestructura on premise, y realizó análisis de vulnerabilidades de seguridad a los activos de información a su infraestructura On Premise.

El segundo subíndice corresponde a Implementación Lineamientos de Política (Ind. 23) que registra un aumento de 1.85 puntos, respecto de la vigencia 2023. Esto se explica porque la gran mayoría de entidades contó con una política o lineamientos definidos y documentados para la generación y restauración de copias de respaldo de la información.

El tercer subíndice corresponde a Asignación de recursos (Ind. 22) que registra un aumento de 5.33 puntos, respecto de la vigencia 2023, el cual se explica por un mayor presupuesto asignado por las entidades distritales a la ciberseguridad, para la protección de los datos digitales en la entidad (costos de personal, herramientas, ips/ids, firewall, antivirus, edr, servidores, sistemas, licencias etc.



Gráfica 3. Puntaje promedio de subíndices de Seguridad Digital 2024



Fuente: Visor resultados IDI – Secretaría General

Al comparar los subíndices de la Política de Seguridad Digital entre 2023 y 2024, se evidencia una mejora en los tres indicadores evaluados, reflejada en una variación promedio de +3,50 puntos. Este incremento se debe al fortalecimiento de la trazabilidad y seguimiento de acciones, la existencia de evidencias más completas y documentadas, y a una mayor articulación entre las áreas para la gestión de la seguridad digital. En términos prácticos, se pasó de cumplir los requisitos a demostrar el cumplimiento con información verificable, lo que evidencia una mayor madurez en la gestión y ejecución de la política.

3. Recomendaciones emitidas por el DAFP

De acuerdo con el análisis nacional de la política, el Departamento Administrativo de la Función Pública (DAFP) identificó las siguientes oportunidades de mejora para el Distrito Capital:

- Recomendación 1: Designar un área o responsable de Seguridad Digital en cada entidad del Distrito que lidere la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) y articule las acciones de mejora institucional, con el fin de mantener



y superar el puntaje de 88,38 alcanzado por la Alcaldía Mayor, fortaleciendo la gobernanza y el seguimiento de los riesgos cibernéticos.

- Recomendación 2: Analizar los incidentes de seguridad digital (ciberseguridad) ocurridos en los distintos sectores y adoptar medidas técnicas, administrativas y de talento humano que garanticen la incorporación de la seguridad digital dentro de los planes sectoriales de gestión y desempeño, de forma que los sectores con menor avance (Ambiente, Cultura y Deporte) cierren brechas frente a los más maduros.
- Recomendación 3: Realizar pruebas de recuperación y restauración de los sistemas de información críticos de cada entidad, verificando la efectividad de los controles implementados y la trazabilidad de los procedimientos de respaldo. Los resultados deben ser evaluados por el Comité de Gestión y Desempeño Institucional, fortaleciendo la capacidad de respuesta ante incidentes digitales.
- Recomendación 4: Contar con un Plan de Recuperación de Desastres (DRP) definido, documentado, probado e implementado para todos los procesos críticos, alineado con el Plan de Continuidad del Negocio (BCP) y los lineamientos del MSPI. Este plan debe garantizar la restauración oportuna de los servicios esenciales y minimizar el impacto operativo frente a eventos de ciberseguridad o fallas tecnológicas.

Estas recomendaciones constituyen la base para el ajuste del plan marco de política, el acompañamiento a las entidades y la definición de acciones de fortalecimiento para la vigencia 2025.

4. Recomendaciones a las entidades del Distrito Capital

Con el propósito de fortalecer la implementación de la política y mejorar los resultados en la próxima medición, se recomienda a las entidades distritales:



1. Fortalecer la Gobernanza de Seguridad Digital

Consolidar un modelo de gobernanza distrital unificado, liderado por la Consejería TIC, que permita coordinar las acciones entre entidades, compartir información sobre incidentes y alinear los recursos técnicos y financieros.

Objetivo: Garantizar decisiones centralizadas, coherencia en los controles y madurez homogénea entre sectores.

2. Designar Responsables Institucionales de Seguridad Digital

Asegurar que todas las entidades distritales cuenten con un responsable formal o área de seguridad digital, con funciones definidas en el Manual de Roles y competencias certificadas conforme al Modelo de Seguridad y Privacidad de la Información (MSPI).

Objetivo: Facilitar la trazabilidad de acciones, la gestión de riesgos y la comunicación con el equipo transversal de seguridad digital del Distrito.

3. Estandarizar la Gestión de Incidentes Digitales

Formalizar un procedimiento distrital de gestión de incidentes, con reporte unificado hacia el CSIRT Distrital y trazabilidad de respuesta y lecciones aprendidas.

Objetivo: Fortalecer la capacidad de reacción, coordinación y mitigación de impactos operacionales y reputacionales.

4. Crear un Esquema de Evaluación de Madurez y Seguimiento

Adoptar una metodología distrital de evaluación de madurez en seguridad digital, basada en los tres subíndices del FURAG (Recursos, Lineamientos, Controles), con revisiones anuales por sector.

Objetivo: Medir la evolución del cumplimiento, priorizar inversiones y sostener la mejora continua.



5. Potenciar la Cultura de Seguridad Digital y Concientización

Diseñar un programa anual de formación y cultura digital para servidores y contratistas, basado en los riesgos del entorno y en la gestión responsable de datos.

Objetivo: Construir una cultura de corresponsabilidad y reducir el factor humano como causa de incidentes de seguridad.