INFORME EJECUTIVO DE DESEMPEÑO DISTRITAL 2025

Política de Seguridad Digital

Secretaría General Oficina Consejería Distrital de Tecnologías de la Información y las Comunicaciones (TIC)

Frederick Sanchez Neira
fsanchez@alcaldiabogota.gov.co

Fecha: Julio, 2026

Resumen ejecutivo

La Política de Seguridad Digital del Distrito Capital mantiene una tendencia positiva en la medición del Índice de Desempeño Institucional 2025, al alcanzar 89,71 puntos y registrar un incremento de 3,45 puntos frente a 2024. Este resultado confirma avances relevantes en despliegue de controles, implementación de lineamientos y fortalecimiento de la capacidad institucional para proteger la información pública y los activos digitales.

El desempeño evidencia una mejora generalizada: 31 de 50 entidades evaluadas se ubicaron en rangos iguales o superiores a 90 puntos, mientras que las entidades con puntajes inferiores a 70 se redujeron de cinco a dos. No obstante, persisten brechas estructurales asociadas principalmente a la asignación de recursos, la continuidad operativa, la gestión de incidentes y la estabilidad de capacidades técnicas en entidades con menor madurez.

Para la alta dirección, el principal reto consiste en consolidar los avances logrados mediante decisiones de priorización presupuestal, fortalecimiento de responsables institucionales, operación efectiva del CSIRT Distrital y seguimiento focalizado a las entidades y sectores con rezagos o retrocesos. La sostenibilidad de la mejora dependerá de pasar de acciones de cumplimiento a un modelo de gobernanza, resiliencia y gestión preventiva de riesgos digitales.

Resultado	Implicación directiva
89,71 puntos en 2025, con mejora de +3,45 frente a 2024.	El Distrito se aproxima a una franja de madurez alta, pero requiere sostener inversiones y capacidades.
El subíndice de Asignación de Recursos permanece como el más bajo.	Se requiere priorización presupuestal para talento, herramientas, continuidad, respaldo y monitoreo.
Las recomendaciones del DAFP se concentran en incidentes, responsables, BCP/DRP y recuperación.	Las acciones 2026–2027 deben enfocarse en resiliencia operativa, gobernanza y seguimiento verificable.
Persisten rezagos y retrocesos en entidades específicas.	Se recomienda acompañamiento focalizado y planes de choque con indicadores semestrales.

1. Introducción

El presente informe presenta los resultados de la Política de Gestión y Desempeño de Seguridad Digital, en el marco de la medición del Índice de Desempeño Institucional (IDI) Vigencia 2025, realizada por el Departamento Administrativo de la Función Pública (DAFP) y publicada en junio de 2026.

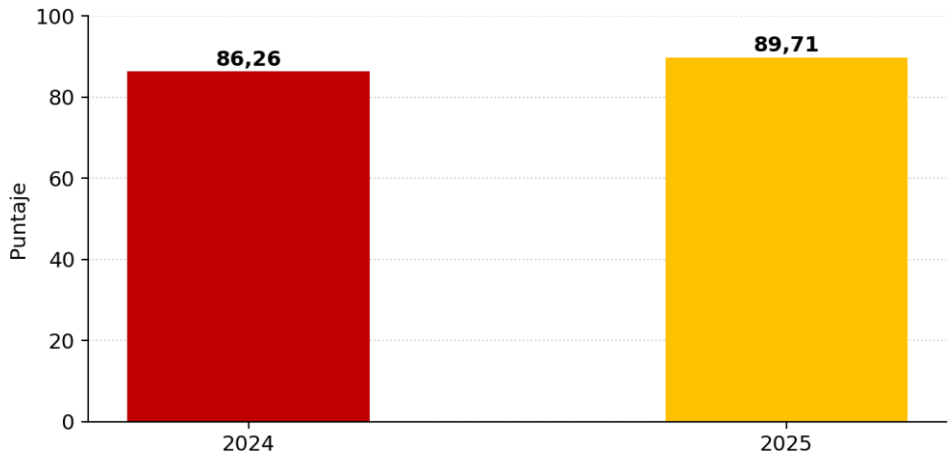
El propósito es consolidar los principales hallazgos, avances, brechas y recomendaciones orientadas a fortalecer la implementación de la política en las entidades del Distrito Capital, bajo los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG) y el compromiso institucional con la mejora continua, la transparencia y la eficiencia de la gestión pública.

El documento integra el análisis comparativo 2024 2025 de los resultados obtenidos por las entidades y sectores administrativos del Distrito, examina el comportamiento de los subíndices que estructuran la política, analiza las recomendaciones emitidas por el DAFP 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 2025

En la medición del Índice de Desempeño Institucional (IDI) 2025, la política de seguridad digital alcanzó un promedio de **89,71 puntos**, lo que representa un incremento de **3,45 puntos** frente a los 86,26 obtenidos en la vigencia 2024 y consolida dos años consecutivos de mejora (82,76 en 2023). Este resultado se enmarca en un desempeño institucional destacado del Distrito, cuyo IDI promedio llegó a 93,8 puntos, superando los promedios de la Nación (88,7), de las gobernaciones (83,7) y de las alcaldías (70,2). (Ver gráfica 1)

GRÁFICA 1
PUNTAJE ÍNDICE DE SEGURIDAD DIGITAL 2024 2025



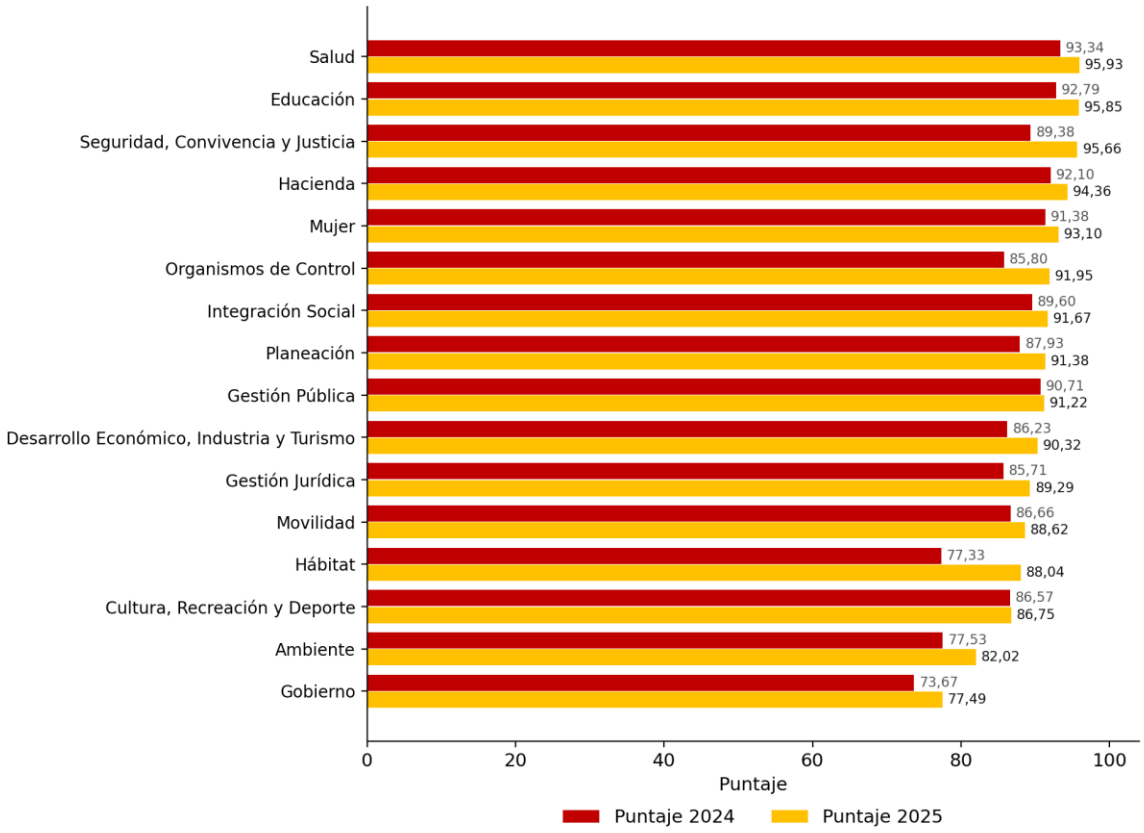
El resultado refleja como fortaleza principal el despliegue de controles técnicos y la implementación de los lineamientos de la política, y confirma que la asignación de recursos, si bien mejora, continúa siendo el eslabón con mayor espacio de crecimiento para consolidar los avances en la siguiente medición.

Desempeño por sector

Desagregado por sectores, el sector con puntaje más alto es **Salud, con 95,93 puntos**, seguido muy de cerca por Educación (95,85) y Seguridad, Convivencia y Justicia (95,66), este último con un avance de 6,28 puntos frente a la medición anterior. El mayor crecimiento sectorial lo registra **Hábitat, con +10,71 puntos** (de 77,33 a 88,04), impulsado por la mejora de varias de sus entidades adscritas y vinculadas. (Ver gráfica 2)

En el extremo opuesto, los sectores **Gobierno (77,49)** y **Ambiente (82,02)** permanecen por debajo del promedio distrital, aun cuando ambos mejoran frente a 2024 (+3,82 y +4,49 puntos, respectivamente). El sector Cultura, Recreación y Deporte se mantiene prácticamente estable (+0,18), lo que exige un acompañamiento diferenciado, dado que concentra las entidades con los mayores retrocesos individuales de la vigencia.

GRÁFICA 2
RANKING POR SECTOR ADMINISTRATIVO ÍNDICE DE SEGURIDAD DIGITAL 2024 2025



Desempeño por subíndices

Esta política se compone de subíndices que corresponden a los elementos estructurales que la conforman y que se visualizan en la gráfica 3. Al comparar 2024 y 2025 se evidencia mejora en los tres:

- El primer subíndice corresponde a **Despliegue de Controles (Ind. 24)**, que pasa de 97,07 a 98,86 puntos, con un aumento de 1,79. Es el subíndice más alto y cercano al óptimo: la gran mayoría de entidades documentó e implementó procedimientos de copias de respaldo y restauración almacenadas en un segmento de red aislado, contó con seguridad perimetral para su infraestructura on premise y realizó análisis de vulnerabilidades sobre sus activos de información.
- El segundo subíndice corresponde a **Implementación de Lineamientos de Política (Ind. 23)**, que pasa de 85,94 a 90,28 puntos, con un aumento de 4,34, el mayor de los tres. Se explica porque más entidades formalizaron políticas y lineamientos documentados para la generación y restauración de copias de respaldo, la gestión de incidentes y la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

- El tercer subíndice corresponde a **Asignación de Recursos (Ind. 22)**, que pasa de 80,88 a 83,96 puntos, con un aumento de 3,08, explicado por un mayor presupuesto asignado por las entidades distritales a la ciberseguridad para la protección de los datos digitales (costos de personal, herramientas, IPS/IDS, firewall, antivirus, EDR, servidores, sistemas y licencias). No obstante, continúa siendo el subíndice más bajo y la principal brecha estructural de la política.

GRÁFICA 3
PUNTAJE PROMEDIO DE SUBÍNDICES DE SEGURIDAD DIGITAL 2025 VS 2024

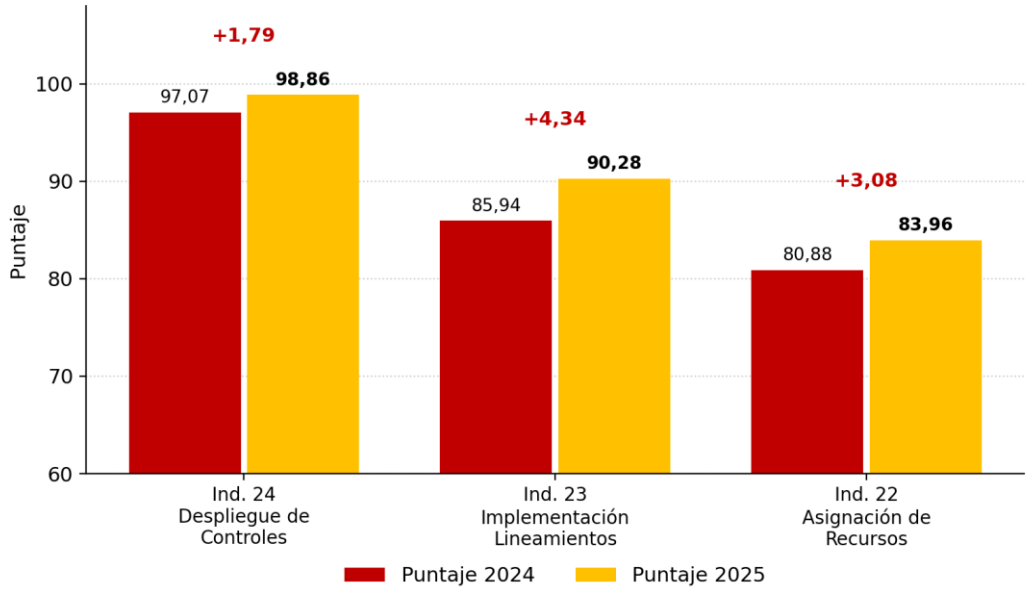


TABLA 1. COMPARATIVO DE SUBÍNDICES 2024 2025

Subíndice	Puntaje 2024	Puntaje 2025	Variación
Ind. 24 Despliegue de Controles	97,07	98,86	**+1,79**
Ind. 23 Implementación Lineamientos de Política	85,94	90,28	**+4,34**
Ind. 22 Asignación de Recursos	80,88	83,96	**+3,08**
Índice de Seguridad Digital (POL08)	**86,26**	**89,71**	**+3,45**

Al comparar los subíndices de la Política de Seguridad Digital entre 2024 y 2025 se evidencia una mejora en los tres indicadores evaluados, reflejada en una variación promedio de +3,45 puntos en el índice. Este incremento se debe al fortalecimiento de la trazabilidad y seguimiento de acciones, la existencia de evidencias más completas y documentadas, y una mayor articulación entre las áreas para la gestión de la seguridad digital. En términos prácticos, las entidades pasaron 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.

Desempeño por entidad

De las 50 entidades y organismos distritales evaluados, **31 (62 %) obtuvieron 90 o más puntos** en 2025, frente a 22 (44 %) en 2024, y las entidades con puntajes inferiores a 70 se redujeron de 5 a 2. Dos entidades alcanzaron el puntaje máximo de 100: la Unidad Administrativa Especial de Servicios Públicos UAESP y la Subred Integrada de Servicios de Salud Norte. (Ver gráfica 4)

GRÁFICA 4
DISTRIBUCIÓN DE ENTIDADES POR RANGO DE PUNTAJE

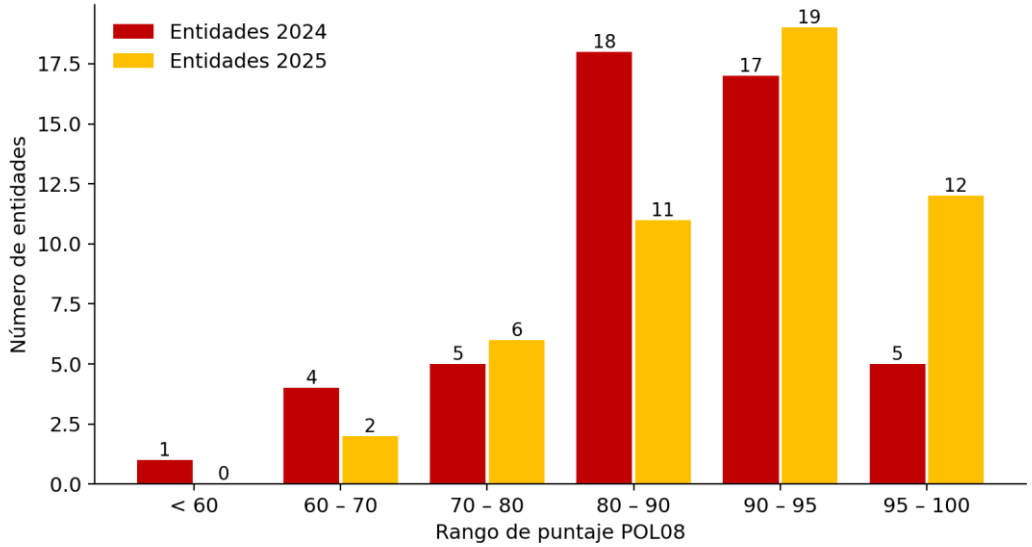
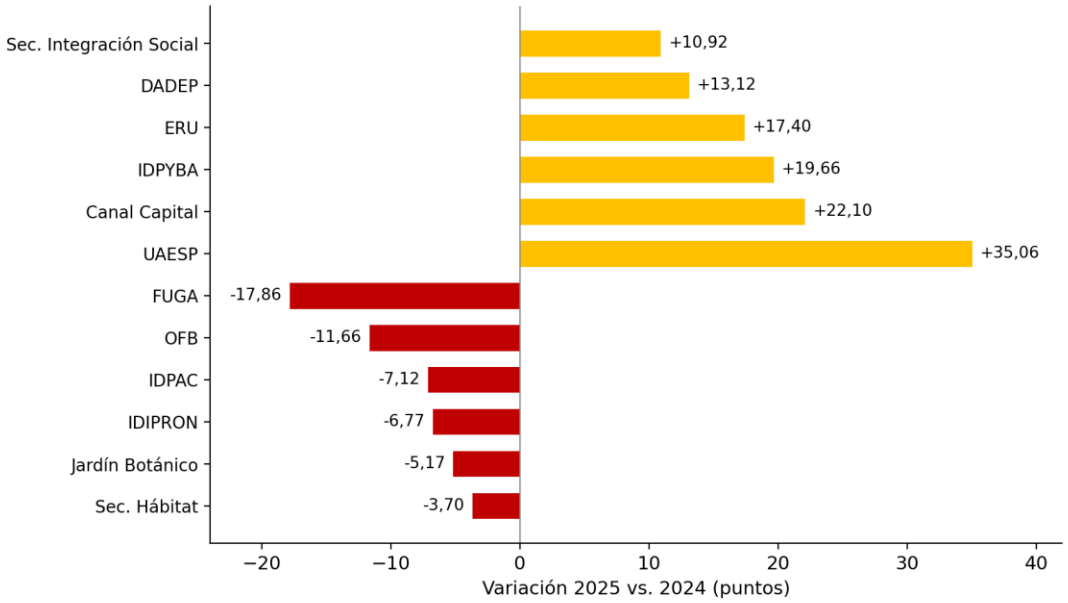


TABLA 2. ENTIDADES CON MEJOR DESEMPEÑO 2025

Entidad	Puntaje 2025
UAE de Servicios Públicos UAESP	**100,00**
Subred Integrada de Servicios de Salud Norte	**100,00**
Secretaría de Educación del Distrito	**98,28**
Instituto Distrital de Recreación y Deporte IDRD	**98,21**
Capital Salud EPS-S S.A.S.	**98,21**
UAE Cuerpo Oficial de Bomberos de Bogotá	**98,21**
UAE de Catastro Distrital	**96,55**
Instituto para la Economía Social IPES	**96,43**
Caja de la Vivienda Popular	**96,43**
Secretaría Distrital de Hacienda	**96,43**

En cuanto a la dinámica interanual, la **UAESP registró el mayor avance del Distrito (+35,06 puntos)**, seguida por Canal Capital (+22,10), el Instituto Distrital de Protección y Bienestar Animal (+19,66) y la Empresa de Renovación y Desarrollo Urbano (+17,40). En contraste, se identifican retrocesos relevantes en la Fundación Gilberto Alzate Avendaño (–17,86), la Orquesta Filarmónica de Bogotá (–11,66) y el IDPAC (–7,12), que con 66,09 puntos presenta el resultado más bajo de la medición y concentra, además, el mayor número de recomendaciones del DAFP en esta política. (Ver gráfica 5)

GRÁFICA 5
MAYORES VARIACIONES POR ENTIDAD 2025 VS. 2024 (PUNTOS)



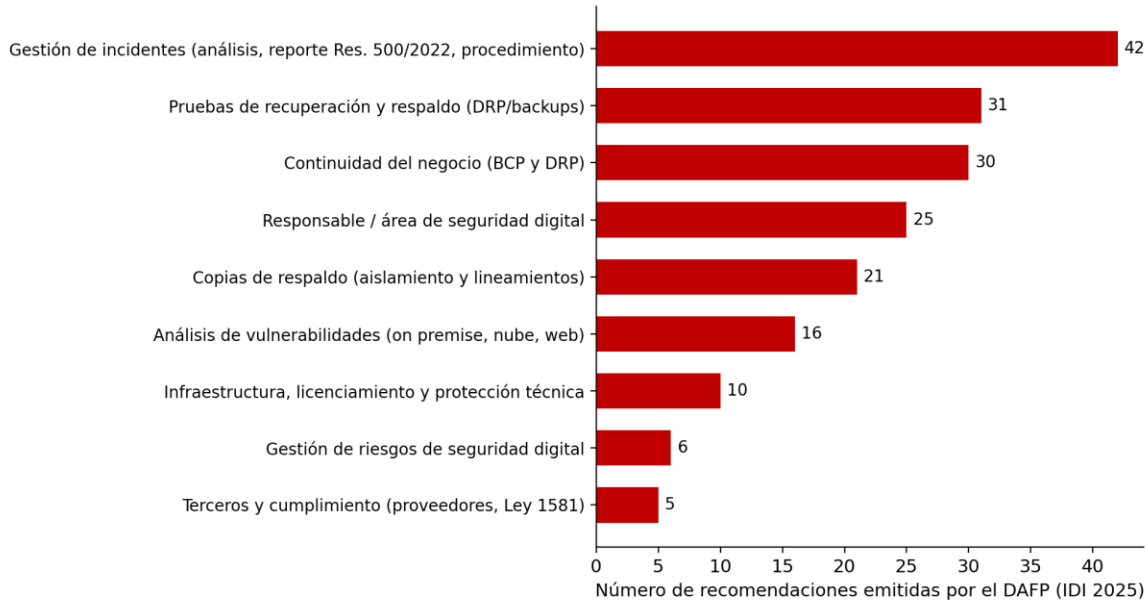
Como gerencia de la política, este comportamiento evidencia dos fenómenos simultáneos: un cierre de brechas en la base (menos entidades rezagadas y mayor concentración en los rangos altos) y, a la vez, una volatilidad en entidades de menor tamaño —principalmente del sector Cultura— asociada a rotación de personal técnico, limitaciones presupuestales y debilidades en la continuidad de los controles implementados, lo que deberá gestionarse con acompañamiento focalizado durante la vigencia 2026.

3.Recomendaciones emitidas por el DAFP

De acuerdo con el análisis nacional de la política, el DAFP emitió 186 recomendaciones de seguridad digital para 49 entidades del Distrito Capital, agrupadas en 22 tipologías. Las entidades con mayor número de recomendaciones son el IDPAC (11), la Fundación Gilberto

Alzate Avendaño, la Orquesta Filarmónica de Bogotá y la Universidad Distrital (9 cada una), en plena correspondencia con los puntajes más bajos de la medición. Las temáticas se concentran en: (Ver gráfica 6)

GRÁFICA 6
RECOMENDACIONES DAFP DE SEGURIDAD DIGITAL POR TEMÁTICA IDI 2025



Las principales recomendaciones formuladas por el DAFP para el Distrito Capital son:

- **Recomendación 1:** Analizar los incidentes de seguridad digital (ciberseguridad) que se presentaron y adoptar medidas técnicas, administrativas y de talento humano que garanticen su incorporación al plan de seguridad y privacidad de la información, mitigando los riesgos relacionados con la protección y privacidad de la información (27 entidades).
- **Recomendación 2:** Designar de manera clara un área o responsable de la seguridad digital que lidere la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) (25 entidades).
- **Recomendación 3:** Realizar pruebas de recuperación de cada uno de los sistemas de información críticos, así como pruebas programadas de respaldo a las copias de seguridad para asegurar la disponibilidad de los datos ante eventos de ransomware (23 entidades).
- **Recomendación 4:** Contar con un Plan de Continuidad del Negocio (BCP) y un Plan de Recuperación de Desastres (DRP) definidos, documentados, probados e implementados para los procesos críticos y misionales (15 entidades cada uno).

- **Recomendación 5:** Fortalecer el esquema de copias de respaldo: separar los equipos que las realizan, almacenarlas en un lugar aislado en un segmento de red diferente al de servidores y equipos, y documentar los lineamientos de generación y restauración (21 entidades).

- **Recomendación 6:** Reportar los incidentes de seguridad digital conforme a la Resolución 500 de 2022 y establecer un procedimiento de gestión de incidentes que incluya la notificación al CSIRT Gobierno / ColCERT (15 entidades).

Estas recomendaciones constituyen la base para el ajuste del plan marco de la política, el acompañamiento a las entidades y la definición de acciones de fortalecimiento para la vigencia 2026 2027.

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:

- **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 de ciberseguridad.

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

- **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 MSPI, manteniendo actualizada la matriz distrital de responsables.

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

- **Estandarizar la Gestión de Incidentes Digitales**

Formalizar un procedimiento distrital de gestión de incidentes, con reporte unificado hacia el CSIRT Distrital conforme a la Resolución 500 de 2022, trazabilidad de respuesta y lecciones aprendidas.

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

- Cerrar la brecha de Asignación de Recursos (Ind. 22)

Incluir en los anteproyectos de presupuesto 2027 partidas específicas para ciberseguridad (talento humano especializado, licenciamiento, EDR, seguridad perimetral, autenticación de correo DMARC/DKIM/SPF y aseguramiento de nube), priorizando las entidades con puntajes inferiores a 80 puntos.

Objetivo: Sostener los controles desplegados y reducir la dependencia de esfuerzos coyunturales, atacando el subíndice de menor desempeño.

- Garantizar la Continuidad y Recuperación Tecnológica (BCP DRP)

Definir, documentar, probar e implementar los planes de continuidad del negocio y de recuperación de desastres para todos los procesos críticos, con pruebas de restauración periódicas, registro de tiempos de recuperación y copias de respaldo aisladas de la red de producción.

Objetivo: Asegurar la resiliencia operativa del Distrito frente a eventos de ransomware, fallas mayores o desastres.

- 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 semestrales para las entidades con retrocesos o puntajes inferiores al promedio distrital.

Objetivo: Medir la evolución del cumplimiento, priorizar inversiones y sostener la mejora continua evitando la volatilidad observada en la vigencia 2025.

- 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, la gestión responsable de datos y la verificación del cumplimiento de las políticas internas de ciberseguridad por parte de proveedores y terceros.

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

5.Estrategias y acciones de fortalecimiento 2026 2027

En su calidad de líder de la política, la Secretaría General - Consejería Distrital de TIC estructuró en el Plan Marco del MIPG 2026 2027 tres acciones estratégicas que responden directamente a las brechas identificadas en la medición:

- **Despliegue del CSIRT Distrital:** contratación y puesta en operación del CSIRT DC, actualización de su portafolio de servicios y modelo de operación, suscripción de acuerdos de cooperación con entidades nacionales e internacionales (ecosistemas FIRST/CSIRT) y emisión periódica de boletines de inteligencia de amenazas (Threat Intelligence Report) orientados a las entidades distritales.
- **Gestión de continuidad:** mantenimiento actualizado de la matriz de responsables de seguridad digital de cada entidad, análisis de incidentes con planes de acción y lecciones aprendidas, ejecución de pruebas de recuperación (DRP) de sistemas críticos con documentación de resultados y tiempos de recuperación, e implementación formal de los planes de recuperación de desastres.

- **Protección de infraestructuras críticas cibernéticas:** identificación y caracterización de las superficies de ataque de las entidades priorizando activos críticos, realización de talleres de cibercrisis con líderes técnicos y de negocio, y ejecución de simulacros de ciberataques (ejercicios tabletop y prácticos) sobre los servicios esenciales del Distrito.

Estas acciones se complementan con la estrategia «Contestemos bien el FURAG», liderada por el Equipo Técnico de Gestión y Desempeño de la CIGD, que contribuyó a la calidad y verificabilidad de las evidencias reportadas en la vigencia 2025, y con el seguimiento semestral del plan de trabajo aprobado en la cuarta sesión del Equipo Técnico realizada el 14 de julio de 2026.

Conclusiones ejecutivas

1. El avance de la Política de Seguridad Digital es significativo y confirma una mejora sostenida del Distrito; sin embargo, el resultado todavía requiere consolidación para superar de manera estable la barrera de 90 puntos.
2. La asignación de recursos es la principal decisión estratégica pendiente: sin presupuesto, talento especializado y herramientas sostenibles, los controles existentes pueden perder efectividad en la siguiente vigencia.
3. La operación del CSIRT Distrital, la gestión de incidentes y las pruebas de continuidad y recuperación deben convertirse en prioridades institucionales, no solo técnicas.
4. Las entidades con retrocesos o puntajes bajos requieren intervención focalizada, seguimiento semestral y planes de choque con responsables, metas y evidencias verificables.
5. La alta dirección debe orientar la política hacia un modelo de madurez digital basado en gobernanza, resiliencia, prevención de riesgos y mejora continua.

Conclusiones detalladas

- La Política de Seguridad Digital consolida una tendencia sostenida de mejora: 82,76 (2023), 86,26 (2024) y 89,71 (2025), con avances en los tres subíndices y una reducción significativa de entidades rezagadas. El Distrito se acerca a la franja de madurez alta (90+) como promedio general.
- El subíndice de Asignación de Recursos (83,96) continúa siendo la brecha estructural de la política; su cierre requiere decisiones presupuestales explícitas en las vigencias 2026 y 2027, especialmente en las entidades y sectores por debajo del promedio (Gobierno, Ambiente y Cultura).
- El desempeño sectorial es cada vez más homogéneo, pero persiste volatilidad en entidades de menor tamaño: los retrocesos de FUGA, OFB e IDPAC concentran el riesgo de la próxima medición y deben ser objeto de planes de choque con acompañamiento directo del líder de política.
- Las 186 recomendaciones del DAFP se concentran en gestión de incidentes, designación de responsables, pruebas de recuperación y continuidad (BCP/DRP): las mismas temáticas que estructuran el Plan Marco 2026 2027, lo que confirma la pertinencia de las acciones estratégicas definidas (CSIRT DC, continuidad e infraestructuras críticas).
- La operación del CSIRT Distrital, la gestión de la matriz de responsables y los ejercicios de cibercrisis y simulacros serán los principales habilitadores para sostener la mejora en la medición de la vigencia 2026, junto con el reporte oportuno de incidentes conforme a la Resolución 500 de 2022.