Documento de recomendaciones para la integración de Gestión de Datos y Seguridad de la Información

CONTENIDO

1. Objetivo 2
2. Marco normativo 2
3. Implementación obligatoria del MSPI y controles de seguridad 12
4. Modelo de gobernanza compartida entre Gestión de Datos y Seguridad de Información ...19
5. Operación y gobernanza de la gestión de incidentes 22
6. Gestión integral de riesgos y resiliencia distrital 28
7. Interoperabilidad segura y el territorio inteligente 34
8. Gestión responsable de datos, transparencia y tecnologías emergentes 39
9. Conclusiones estratégicas de alineación institucional 44
10. Hoja de Ruta estratégica para la implementación 49

1. OBJETIVO

Brindar los lineamientos estratégicos y operativos para las 63 Entidades del Distrito, alineados con el Plan Distrital de Desarrollo *"Bogotá Camina Segura"* y con los marcos normativos nacionales y distritales aplicables, con el propósito de fortalecer la integración entre la gestión de datos, la seguridad de la información y la privacidad.

De esta manera, se promueve la transición progresiva hacia un territorio inteligente, seguro, interoperable y resiliente.

Las recomendaciones contenidas en este documento se fundamentan en tres insumos diagnósticos complementarios:

1) El *Análisis del Diagnóstico de Madurez y Mapa Operativo de Capacidades para la Alcaldía de Bogotá*, el cual identifica patrones, brechas transversales, capacidades críticas a intervenir y define un esquema de "Mínimo Viable Operativo" (MVO) diferenciado según los grupos de madurez identificados.

2) Los resultados de la categoría de Seguridad y Privacidad de la Información (Paquete 4) de la Herramienta de Medición de Madurez de Capacidades para Implementar la Infraestructura de Datos del Distrito (IDD), aplicados a las Entidades distritales conforme a los lineamientos establecidos por el Departamento Nacional de Planeación (DNP).

3) El diagnóstico de ciberseguridad realizado por el equipo de Ciberseguridad del Distrito en el 2025.

La integración de estas tres fuentes permite formular las recomendaciones alineadas con la realidad institucional del Distrito, sustentadas en evidencia objetiva y orientadas a fortalecer las capacidades de manera gradual, proporcional y sostenible.

2. MARCO NORMATIVO

A continuación, se presenta un resumen detallado de las principales fuentes normativas, estratégicas y técnicas consultadas, las cuales constituyen el marco de referencia para el fortalecimiento de la gestión de datos, la seguridad de la información, la privacidad y la transformación digital en las Entidades del Distrito Capital.

Este marco integra lineamientos nacionales y distritales orientados a promover una gestión segura, interoperable, ética y sostenible de la información, así como el desarrollo progresivo de capacidades institucionales:

1. Acuerdo 927 de 2024: Plan Distrital de Desarrollo "Bogotá Camina Segura"

El Acuerdo 927 de 2024 adopta el Plan Distrital de Desarrollo 2024–2027 "Bogotá Camina Segura", el cual establece la hoja de ruta estratégica de la actual administración distrital y define las principales prioridades de gestión pública para el período.

El Plan se estructura sobre cinco (5) objetivos estratégicos:

1) **Bogotá avanza en seguridad:**
Orientado al fortalecimiento de la seguridad, la convivencia, el orden público y la justicia mediante el uso estratégico de tecnologías y capacidades digitales.

2) **Bogotá confía en su Bien-estar:**
Enfocado en la reducción de la pobreza, la seguridad alimentaria, el fortalecimiento del sistema de salud y los programas sociales para todos.

3) **Bogotá confía en su potencial:**
Promueve la educación, la innovación, la transformación digital y la consolidación de Bogotá como un ecosistema de conocimiento y desarrollo tecnológico.

4) **Bogotá ordena su territorio:**
Prioriza la movilidad sostenible, la planeación territorial, la gestión ambiental y el fortalecimiento de capacidades institucionales para la gestión del riesgo y la resiliencia urbana.

5) **Bogotá confía en su gobierno:**
Impulsa un modelo de gestión pública basado en la transparencia, la integridad, la apertura institucional y el aprovechamiento estratégico de los datos para mejorar la toma de decisiones y los servicios al ciudadano.

2. Decreto 640 de 2025: Decreto único del sector Gestión Pública

El Decreto 640 de 2025 tiene como propósito compilar y armonizar la normativa vigente asociada al Sector de Gestión Pública del Distrito Capital, con el objeto de fortalecer la coordinación institucional, la eficiencia administrativa y la articulación de políticas transversales entre las Entidades distritales.

Para efectos del presente documento, tienen especial relevancia los siguientes títulos:

- **Título 7 – Componentes de la Infraestructura de Datos y Modelo de Gobernanza correspondiente en el Distrito Capital:**
Define los componentes, roles, responsabilidades y mecanismos de coordinación requeridos para la gobernanza de la Infraestructura de Datos del Distrito, constituyéndose en el marco institucional que orienta la gestión, calidad, intercambio y aprovechamiento estratégico de los datos.

- **Título 8 – Modelo de Gobernanza de Seguridad Digital para el Distrito:**
Define el marco institucional para la implementación de la política de seguridad digital en las Entidades distritales, incluyendo los roles, responsabilidades, instancias de coordinación, gobernanza, esquemas de articulación interinstitucional y criterios para la adopción de controles y capacidades de seguridad.

En consecuencia, los lineamientos, recomendaciones y acciones propuestas en el presente documento deberán implementarse de manera articulada con los modelos de gobernanza definidos en ambos títulos, garantizando la coherencia entre la gestión de datos, la seguridad digital, la estructura institucional vigente y las capacidades operativas del ecosistema distrital.

3. Lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI)

Los Lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI), definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), establecen el marco de referencia para la implementación y fortalecimiento de Sistemas de Gestión de Seguridad y Privacidad de la Información (SGSPI) en las Entidades públicas.

El MSPI se encuentra alineado con estándares internacionales como ISO/IEC 27001:2022 y adopta un enfoque de mejora continua basado en el ciclo PHVA (Planear, Hacer, Verificar y Actuar), estructurado en las siguientes cinco (5) fases:

1) **Diagnóstico:**
   Identificación del estado actual de la Entidad mediante análisis de brechas, evaluación de capacidades y revisión de controles existentes.

2) **Planificación:**
   Definición del alcance del modelo, establecimiento de responsabilidades, identificación de activos de información y valoración de riesgos de seguridad y privacidad.

3) **Operación:**
   Implementación de controles técnicos, organizacionales y procedimentales orientados a proteger la confidencialidad, integridad y disponibilidad de la información.

4) **Evaluación del desempeño:**
   Seguimiento y medición de la eficacia de los controles implementados mediante auditorías, indicadores y mecanismos de monitoreo.

5) **Mejoramiento continuo:**
   Definición de acciones correctivas y oportunidades de mejora para fortalecer progresivamente el sistema de gestión y su capacidad de respuesta frente a riesgos e incidentes.

4. Estrategia Distrital de Ciberseguridad (CINTEL)

La Estrategia Distrital de Ciberseguridad, desarrollada con el apoyo de CINTEL, constituye el marco de referencia para fortalecer las capacidades de ciberseguridad, resiliencia digital y continuidad operativa de las Entidades del Distrito Capital, frente al incremento de riesgos y amenazas sobre los activos digitales y la infraestructura tecnológica institucional.

Se articula en nueve (9) componentes fundamentales, donde se destacan:

- **Gobernanza y marco estratégico:**
  Define los lineamientos de coordinación institucional, roles y mecanismos de articulación para fortalecer la gestión distrital de la ciberseguridad y su alineación con las políticas nacionales y distritales de seguridad digital.

- **Gestión de riesgos y protección de activos:**
  Promueve la identificación, valoración y mitigación de riesgos asociados a los activos de información, servicios digitales e infraestructuras tecnológicas críticas del Distrito.

- **Monitoreo, detección y respuesta ante incidentes:**
  Fortalece las capacidades distritales de monitoreo y gestión de incidentes mediante la articulación del SOC Distrital y el CSIRT Distrital, permitiendo mejorar la capacidad de detección, análisis, contención y respuesta frente a eventos de ciberseguridad.

- **Continuidad operativa y recuperación:**
  Impulsa la adopción de estrategias de continuidad del negocio, recuperación ante desastres y restauración de servicios críticos, mediante planes de continuidad operativa (BCP) y recuperación tecnológica (DRP).

- **Desarrollo de capacidades y articulación institucional:**
  Fomenta el intercambio de información, la cooperación interinstitucional y el fortalecimiento de capacidades técnicas y organizacionales en materia de seguridad digital, ciberseguridad y gestión de incidentes.

5. Estrategia Nacional de Seguridad Digital 2025-2027

La Estrategia Nacional de Seguridad Digital 2025-2027 expedida por el Gobierno Nacional, constituye el principal instrumento de política pública en materia de seguridad digital a nivel nacional y define la visión, principios, objetivos y líneas de acción que orientan el fortalecimiento de la ciberseguridad y la resiliencia digital del país.

El Distrito Capital articula sus lineamientos de seguridad digital con esta Estrategia Nacional y los operacionaliza a nivel distrital mediante los instrumentos normativos y de gobernanza vigentes, en particular a través del Modelo de Gobernanza de Seguridad Digital definido en el Título 8 del Decreto Distrital 640 de 2025.

La Estrategia establece cuatro (4) objetivos específicos que resultan especialmente relevantes para alinear los planes distritales con las metas nacionales de manera precisa y medible:

1) **Gobernanza y articulación institucional:**
   Orientado a fortalecer los mecanismos de coordinación nacional e internacional en materia de seguridad digital, promoviendo esquemas de colaboración entre Entidades públicas, el sector privado y organismos internacionales.

2) **Ciber resiliencia y protección de infraestructuras críticas:**
   Promueve la adopción de modelos avanzados de protección, incluyendo arquitecturas de "Confianza Cero" (*Zero Trust*), la gestión proactiva de amenazas y la capacidad de respuesta y recuperación ante incidentes de seguridad digital.

3) **Desarrollo de capacidades y talento especializado:**
   Impulsa estrategias de formación, apropiación social y fortalecimiento de competencias en seguridad digital, tanto en el ámbito técnico como en la cultura organizacional de las Entidades públicas.

4) **Fortalecimiento normativo y ético:**
   Promueve la actualización de los marcos regulatorios asociados al ciberdelito y el uso responsable de tecnologías emergentes, incluyendo lineamientos éticos relacionados con la inteligencia artificial.

Los resultados del diagnóstico de madurez evidencian que, además de los desafíos tecnológicos, persisten brechas relevantes en gobernanza, cultura, apropiación organizacional y desarrollo de capacidades especializadas, que guardan una relación directa con el tercer objetivo de la Estrategia Nacional.

En consecuencia, se recomienda que las Entidades distritales incorporen estos cuatro objetivos como referentes de alineación dentro de sus instrumentos de planeación (PEI, Planes de Acción, PGSPI y demás instrumentos aplicables), priorizando las iniciativas de ciber resiliencia en aquellas Entidades responsables de infraestructuras o servicios críticos (salud, movilidad, hacienda, seguridad) y fortaleciendo el objetivo de desarrollo de capacidades y talento especializado como componente transversal de la gestión del talento humano en todas las Entidades del Distrito.

6. Modelo de Respuesta a Incidentes (CINTEL)

El Modelo de Respuesta a Incidentes constituye un instrumento técnico orientado a fortalecer y estandarizar los procesos de gestión de incidentes de ciberseguridad en Entidades del Distrito Capital.

Su propósito es establecer lineamientos comunes para mejorar la capacidad de preparación, detección, análisis, contención, recuperación y coordinación institucional frente a eventos que puedan comprometer la disponibilidad, integridad o confidencialidad de la información y los servicios digitales distritales. El modelo se encuentra alineado con estándares y buenas prácticas internacionales en materia de gestión de incidentes y resiliencia digital.

Entre sus principales componentes se destacan:

- **Ciclo de vida de gestión de incidentes:**
  Define un modelo integral de atención basado en estándares internacionales como NIST SP 800-61 e ISO/IEC 27035, incorporando fases de preparación, identificación, análisis, contención, erradicación, recuperación y mejora continua frente a incidentes de seguridad digital.

- **Clasificación y priorización de incidentes:**
  Establece criterios de categorización y niveles de severidad (leve, moderado, mayor y crítico) para facilitar la priorización de eventos, la asignación de recursos y la escalabilidad de la respuesta institucional.

- **Guías operativas y protocolos de actuación**:
  Incorpora playbooks o procedimientos específicos para la atención de escenarios de ciberseguridad frecuentes, como ataques de ransomware, fuga de información, accesos no autorizados, indisponibilidad de servicios o incidentes asociados a entornos cloud.

- **Coordinación y escalamiento institucional:**
  Define mecanismos de articulación y escalamiento entre las Entidades distritales, el SOC Distrital, el CSIRT Distrital y el COLCERT, con el propósito de fortalecer la respuesta coordinada frente a incidentes de alto impacto.

7. Modelo de Gestión de Riesgos de Ciberseguridad (CINTEL)

El Modelo de Gestión de Riesgos de Ciberseguridad establece una metodología unificada para que las Entidades distritales identifiquen, evalúen, gestionen y mitiguen los riesgos asociados a la seguridad digital y la protección de sus activos de información.

Asimismo, promueve la adopción de criterios homogéneos de análisis y tratamiento de riesgos dentro del ecosistema distrital, alineados con estándares nacionales e internacionales de gestión de riesgos y seguridad de la información.

Entre sus principales componentes se destacan:

- **Proceso metodológico de gestión de riesgos:**
  Define una metodología estructurada para la identificación de activos críticos, procesos estratégicos, amenazas, vulnerabilidades y escenarios de riesgo asociados a la infraestructura tecnológica y a los servicios digitales institucionales.

- **Valoración y priorización de riesgos:**
  Incorpora los mecanismos de análisis basados en matrices de probabilidad e impacto, alineados con la Guía para la Administración del Riesgo del DAFP (Versión 7) y estándares internacionales como ISO/IEC 27005, permitiendo priorizar los riesgos de acuerdo con su criticidad y nivel de exposición.

- **Tratamiento y mitigación:**
  Establece los lineamientos para definir estrategias de tratamiento de riesgos, incluyendo acciones de mitigación, transferencia, aceptación o evitación, con el propósito de reducir progresivamente los niveles de riesgo residual a rangos aceptables para la Entidad.

- **Gestión de riesgos asociados a terceros:**
  Incorpora criterios específicos para la identificación y control de riesgos relacionados con proveedores, contratistas, servicios tecnológicos externos y cadenas de suministro digital, reconociendo la creciente dependencia de servicios tercerizados dentro de los ecosistemas tecnológicos institucionales.

8. Políticas Distritales de Seguridad Digital (CINTEL)

Las Políticas Distritales de Seguridad Digital constituyen el marco general de lineamientos y directrices que orientan a las Entidades del Distrito Capital en la implementación de medidas de seguridad digital, protección de la información y fortalecimiento de capacidades institucionales frente a riesgos y amenazas cibernéticas.

Entre sus principales componentes se destacan cuatro (4) frentes estratégicos:

1) **Gobernanza, seguimiento y articulación institucional:**
   Define mecanismos de coordinación, responsabilidades institucionales y esquemas de seguimiento para fortalecer la gestión de la seguridad digital en las Entidades distritales, incluyendo la designación de puntos focales y la articulación con instrumentos de reporte y medición institucional como FURAG y MSPI.

2) **Gestión de riesgos de seguridad digital:**
   Establece lineamientos para la identificación, evaluación y tratamiento de riesgos digitales, promoviendo la aplicación de criterios de proporcionalidad, priorización y enfoque basado en riesgos, de acuerdo con la naturaleza misional y el nivel de criticidad de cada Entidad.

3) **Protección de activos de información y datos:**
   Promueve la adopción de medidas de seguridad desde el diseño y durante todo el ciclo de vida de la información, incluyendo controles asociados a cifrado, acceso seguro, protección de datos y administración de infraestructuras tecnológicas.

4) **Gestión y respuesta a incidentes**:
   Define los lineamientos para la detección, reporte, escalamiento y atención de incidentes de seguridad digital, incluyendo obligaciones relacionadas con la notificación temprana de eventos y la preservación de evidencia digital para fines de análisis, investigación y respuesta institucional.

9. Acuerdo 002 de 2025 de la CDTD – Lineamientos de Interoperabilidad del Distrito Capital

El Acuerdo 002 de 2025, expedido por la Comisión Distrital de Transformación Digital (CDTD), establece los lineamientos de interoperabilidad para las Entidades del Distrito Capital desde tres dimensiones: organizacional, técnica y semántica.

Estos lineamientos contemplan aspectos de ciberseguridad directamente relacionados con el uso y aprovechamiento de datos, incluyendo los requisitos de autenticación, autorización, cifrado en tránsito y en reposo, trazabilidad de las transacciones de datos y cumplimiento de las políticas de privacidad en los procesos de interoperabilidad.

El Acuerdo se complementa con los siguientes cinco (5) anexos técnicos que facilitan su implementación operativa y estandarizan mecanismos de intercambio de información entre Entidades:

- **Anexo 1:** Plantilla de acuerdo de confidencialidad e intercambio de información celebrado entre Entidades.
- **Anexo 2:** Anexo Técnico que complementa al Anexo 1 y define las especificaciones de seguridad y calidad del intercambio.
- **Anexo 3:** Perfil del Administrador de Datos, que establece las competencias y responsabilidades del rol clave para la gobernanza del dato en cada Entidad.
- **Anexo 4:** Esquema de gobernanza de interoperabilidad, que define la estructura institucional, los roles, las instancias de coordinación y los mecanismos de seguimiento para la gestión de la interoperabilidad a nivel distrital.
- **Anexo 5:** Lineamientos y especificaciones técnicas para el diseño de APIs y servicios web, los estándares técnicos para la exposición e integración de servicios de interoperabilidad.

La articulación entre estos lineamientos de interoperabilidad y las recomendaciones de seguridad contenidas en el presente documento es esencial para garantizar que el intercambio de información entre Entidades se realice bajo condiciones de confidencialidad, integridad y disponibilidad.

10. Acuerdo 003 de 2025 de la CDTD – Lineamientos y estándares para sistemas de Inteligencia Artificial en el Distrito Capital

El Acuerdo 003 de 2025, expedido por la Comisión Distrital de Transformación Digital (CDTD), establece los lineamientos y estándares para la preparación, desarrollo, implementación, supervisión y mejora continua de los sistemas de Inteligencia Artificial en las Entidades y organismos del Distrito Capital.

Este Acuerdo se complementa con el Anexo de Lineamientos Técnicos y Éticos en IA, el cual define los principios, requisitos técnicos y estándares éticos que deben regir el desarrollo y uso de sistemas de IA en el Distrito.

El Acuerdo 003 de 2025 establece una clasificación de los proyectos de IA en tres niveles de madurez, cada uno con controles, evidencias y responsabilidades específicas:

- **Nivel Exploratorio:** proyectos en fase de idea, prototipo o piloto que utilicen datos no personales o anonimizados y no tomen decisiones administrativas.
- **Nivel Consolidación:** proyectos que utilizan datos reales o institucionales con base jurídica definida y se encuentran en proceso de despliegue o validación ampliada.
- **Nivel Avanzado:** proyectos en operación institucional que procesan datos personales o información sensible o que inciden directamente en decisiones administrativas.

Este marco normativo se articula con el Decreto Distrital 575 de 2023 (actualmente compilado en el Título 7 del Decreto 640 de 2025), que define los componentes de la Infraestructura de Datos y establece el modelo de gobernanza correspondiente, así como con la Política Nacional de Inteligencia Artificial adoptada mediante el CONPES 4144 de 2025, que establece los lineamientos estratégicos para el desarrollo, adopción y uso responsable de sistemas de inteligencia artificial en Colombia.

Las recomendaciones de seguridad y privacidad contenidas en el presente documento se articulan con los lineamientos definidos en estos instrumentos normativos, incorporando buenas prácticas para la protección de los datos, la gestión de riesgos, el control de accesos, la transparencia y el uso responsable de sistemas de inteligencia artificial y otras tecnologías emergentes.

11. Marco de Interoperabilidad del MinTIC y Estándar de Lenguaje Común

El Marco de Interoperabilidad definido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) establece los principios, estándares y directrices para orientar el intercambio seguro y eficiente de información entre Entidades del Estado colombiano.

En este contexto, el Lenguaje Común de Intercambio de Información constituye el referente técnico para la estandarización semántica de los datos intercambiados entre Entidades, promoviendo un entendimiento común sobre la estructura y significado de la información y facilitando la interoperabilidad entre sistemas de información.
En consecuencia, las iniciativas de interoperabilidad promovidas por las Entidades distritales deberán alinearse con los estándares y lineamientos definidos por el Marco de Interoperabilidad y el Lenguaje Común de Intercambio de Información, garantizando la consistencia semántica, la reutilización eficiente de la información y la compatibilidad con los ecosistemas de intercambio de datos del orden nacional.

12. Acuerdo 001 de 2025 del Comité Distrital de Datos – Reglamento Interno

El Acuerdo 001 de 2025, expedido por el Comité Distrital de Datos, adopta el Reglamento Interno de funcionamiento del Comité Distrital de Datos, estableciendo su objeto, integración, esquema de funcionamiento, periodicidad de sesiones, mecanismos de decisión y disposiciones para el seguimiento de las acciones asociadas a la Infraestructura de Datos del Distrito.

El Comité Distrital de Datos constituye la instancia de coordinación interinstitucional del nivel estratégico del componente de Gobernanza de la Infraestructura de Datos del Distrito, cuyo propósito es definir las estrategias y prioridades para el desarrollo y fortalecimiento de los demás componentes de la infraestructura, así como orientar las acciones necesarias para el aprovechamiento de los datos en el Distrito Capital.

En consecuencia, las recomendaciones contenidas en el presente documento, especialmente aquellas relacionadas con gobernanza de datos, calidad de la información, interoperabilidad y fortalecimiento de capacidades institucionales, deberán implementarse de manera articulada con los lineamientos, orientaciones y mecanismos de coordinación definidos por esta instancia.

13. Acuerdo 001 de 2025 de la CDTD – Creación del Grupo de Trabajo de Ciberseguridad

El Acuerdo 001 de 2025, expedido por la Comisión Distrital de Transformación Digital (CDTD), crea el Grupo de Trabajo de Ciberseguridad como un equipo técnico especializado, de carácter asesor y encargado de apoyar la implementación del Modelo de Gobernanza de Seguridad Digital del Distrito, así como de formular recomendaciones sobre políticas, lineamientos, estrategias e iniciativas de ciberseguridad para las Entidades distritales.

Este Grupo constituye un espacio técnico de articulación interinstitucional para el análisis del estado de la ciberseguridad distrital, la identificación de buenas prácticas, la formulación de recomendaciones para el fortalecimiento de capacidades y la definición y mejora continua de los lineamientos y reglamentos operativos asociados al CSIRT Distrital.

Las recomendaciones de seguridad y privacidad contenidas en el presente documento deberán alinearse con los lineamientos, buenas prácticas y orientaciones técnicas promovidas por esta instancia, contribuyendo al fortalecimiento progresivo de las capacidades de seguridad digital en el ecosistema distrital.

14. Decreto 575 de 2023 – Infraestructura de Datos y Modelo de Gobernanza

El Decreto 575 de 2023 definió los componentes de la Infraestructura de Datos del Distrito Capital y estableció el modelo de gobernanza correspondiente, constituyéndose en el principal antecedente normativo para la gestión, intercambio, aprovechamiento y protección de los datos como activo estratégico del Distrito.

Sus disposiciones fueron posteriormente compiladas en el Título 7 – Componentes de la Infraestructura de Datos y Modelo de Gobernanza Correspondiente en el Distrito Capital del Decreto 640 de 2025, por lo que actualmente constituye un referente normativo e histórico para comprender la evolución del modelo distrital de gestión de datos.

Las recomendaciones contenidas en el presente documento se articulan con los lineamientos de gobernanza establecidos en dicho marco normativo, promoviendo el fortalecimiento de capacidades relacionadas con la gestión de datos, la interoperabilidad, la seguridad y privacidad de la información, y el aprovechamiento estratégico de los datos en las Entidades distritales.

15. CONPES 4144 de 2025 – Política Nacional de Inteligencia Artificial

El documento CONPES 4144 de 2025, adopta la Política Nacional de Inteligencia Artificial, estableciendo la hoja de ruta del país para fortalecer las capacidades de investigación, desarrollo, adopción y aprovechamiento ético y sostenible de sistemas de inteligencia artificial, con horizonte al año 2030.

La política se estructura alrededor de 6 ejes relacionados con: 1) Ética y Gobernanza; 2) Datos e Infraestructura; 3) Investigación, Desarrollo e Innovación; 4) Desarrollo de Capacidades y Talento Digital; 5) Mitigación de Riesgos; y 6) Uso y Adopción de la IA, en los sectores público y privado.

Las recomendaciones contenidas en el presente documento se encuentran alineadas con los principios y lineamientos definidos en esta política nacional, particularmente en materia de gobernanza de datos, protección de la información, uso responsable y ético de la inteligencia artificial, gestión de riesgos, fortalecimiento de capacidades institucionales y adopción segura de tecnologías emergentes.

Documentos técnicos de referencia

Adicionalmente al marco normativo descrito, se consideran los siguientes dos (2) insumos técnicos de referencia, cuyos hallazgos y recomendaciones fueron considerados para la formulación de los lineamientos contenidos en el presente documento:

1. Instrumento de Madurez de Capacidades (IMC) para implementar la Infraestructura de Datos del Distrito

El Instrumento de Madurez de Capacidades (IMC), desarrollado por el Departamento Nacional de Planeación (DNP), constituye la herramienta de referencia utilizada para evaluar el nivel de desarrollo de las capacidades necesarias para implementar la Infraestructura de Datos en las Entidades públicas.

El IMC evalúa nueve (9) paquetes de capacidades, entre los cuales se encuentra el *Paquete 4: Seguridad y Privacidad de la Información*, que mide específicamente las capacidades institucionales asociadas a la protección de la información, la gestión de riesgos de seguridad digital, el cumplimiento del MSPI y la adopción de controles de privacidad.

Los resultados de la aplicación del IMC a las Entidades del Distrito Capital, disponibles a través del tablero de control de la *Herramienta de Medición de Madurez de Capacidades para Implementar la Infraestructura de Datos del Distrito (IDD)* (https://gobiernoabiertobogota.gov.co/gab/indice-gobierno-abierto/herramienta-medicion-madurez-capacidades), evidencian que el ecosistema distrital no es homogéneo en materia de seguridad y privacidad y que los niveles de madurez varían significativamente entre Entidades. Esto justifica la adopción de un enfoque diferenciado y proporcional en la implementación de los lineamientos de este documento.

El diagnóstico evidenció las siguientes brechas estructurales prioritarias en el ecosistema distrital:

- **Gestión de datos maestros y referenciales:**
  Los bajos resultados registrados en los atributos de profundidad, alcance y relevancia evidencian una brecha estructural en la gestión de datos maestros y referenciales, considerada una capacidad fundacional para asegurar la consistencia, calidad, estandarización y aprovechamiento de la información en el ecosistema distrital

- **Desarticulación entre arquitectura de datos y gestión documental:**
  Los bajos resultados registrados en capacidades como *"Gestión de arquitectura de datos participativa"* y *"Captura de metadatos automatizada"* evidencian una brecha estructural en la integración entre la arquitectura de datos y la gestión documental, una capacidad fundamental para garantizar la trazabilidad, organización e interoperabilidad de los activos de información del Distrito

- **Informalidad en los acuerdos de intercambio de información:**
  Los bajos resultados registrados en capacidades como *"Acuerdo de Niveles de Servicio (ANS)"* evidencian una brecha estructural en la formalización de los mecanismos de intercambio de información, una capacidad fundamental para garantizar procesos de interoperabilidad seguros, confiables y sostenibles entre las Entidades del Distrito.

La incorporación de este instrumento como marco de referencia técnico permite fundamentar las prioridades definidas en el presente documento sobre evidencia objetiva del estado actual del ecosistema distrital.

En consecuencia, se recomienda que las Entidades prioricen el fortalecimiento de las capacidades fundacionales de gestión y gobierno de datos, reconociendo que estas constituyen la base necesaria para el desarrollo sostenible de capacidades de analítica avanzada e inteligencia artificial.

2. Análisis del Diagnóstico de Madurez y Mapa Operativo de Capacidades para la Alcaldía de Bogotá

El documento de *Análisis del Diagnóstico de Madurez y Mapa Operativo de Capacidades para la Alcaldía de Bogotá* consolida los resultados del IMC aplicado a las Entidades distritales e identifica patrones, brechas transversales y capacidades críticas a intervenir.

A partir de los resultados obtenidos, se clasifican las Entidades en tres (3) grandes grupos:

- **Grupo A – Líderes y pioneros**:
  Entidades que han alcanzado niveles de "Puesta en Marcha" y "Apropiación y Sostenibilidad", demostrando que la institucionalización de los datos es posible en el sector público cuando existe liderazgo institucional y una orientación organizacional basada en información.

- **Grupo B – Instituciones en transición**:
  Es el grupo más numeroso, compuesto por Entidades que han alcanzado el nivel "Exploratorio y emergente", que reconocen el valor del dato y han ejecutado proyectos aislados, sin embargo dependen principalmente de iniciativas individuales en lugar de procesos institucionalizados.

- **Grupo C – Rezagados críticos**:
  Entidades en el nivel “Inicial”, con estados incipientes de institucionalización de capacidades de datos, con limitaciones relevantes en materia de gobernanza, asignación presupuestal, definición de roles y formalización de procesos, que requieren atención prioritaria por el impacto de sus funciones misionales.

El diagnóstico evidencia que las brechas de madurez no solo se presentan entre sectores, sino también al interior de un mismo sector, donde coexisten Entidades con niveles avanzados de madurez junto a Entidades con capacidades incipientes. Este comportamiento demuestra que el desarrollo de capacidades de datos depende más del liderazgo institucional de cada Entidad, que de una adopción homogénea de lineamientos centralizados.

De la misma manera, el análisis recomienda la creación de un esquema de "Mínimo Viable Operativo" (MVO) diferenciado por grupo de madurez, el cual se articula directamente con las recomendaciones de seguridad y privacidad incluidas en este documento.

3. IMPLEMENTACIÓN OBLIGATORIA DEL MSPI Y CONTROLES DE SEGURIDAD

La adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio TIC debe trascender el cumplimiento documental y consolidarse como un componente transversal dentro de la gestión institucional de datos, la arquitectura tecnológica y los procesos operativos de las Entidades distritales.

En este contexto, la seguridad de la información debe entenderse como una capacidad habilitadora del ciclo de vida del dato y no únicamente como una función tecnológica aislada.

Enfoque de proporcionalidad basado en el diagnóstico de madurez

La aplicación de los lineamientos contenidos en esta sección debe realizarse bajo un enfoque de proporcionalidad, fundamentado en los hallazgos del Instrumento de Madurez de Capacidades (IMC) y en los ejercicios de diagnóstico de ciberseguridad realizados en el 2025.

La aplicación de un estándar uniforme de controles de seguridad para todas las Entidades del Distrito resultaría ineficiente, dado que Entidades con capacidades radicalmente distintas no pueden ser evaluadas ni intervenidas bajo los mismos criterios de implementación.

Este enfoque se encuentra alineado con los Lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC y con el estándar ISO/IEC 27001:2022, los cuales establecen que la implementación de controles de seguridad debe responder al contexto organizacional, la valoración de riesgos y los activos de información que se busca proteger.

En consecuencia, la implementación de los controles técnicos, organizacionales y operativos que se describen a continuación deberá considerar el grupo de pertenencia de cada Entidad conforme a la segmentación derivada del IMC:

- **Entidades del Grupo A**:
  Deberán avanzar hacia la implementación de controles avanzados, incluyendo arquitecturas de Confianza Cero, mecanismos de anonimización, automatización de monitoreo y adopción de estándares internacionales de certificación.

  Adicionalmente, deberán asumir un rol activo como Entidades Mentoras, promoviendo la transferencia de buenas prácticas y experiencias exitosas en materia de seguridad, privacidad y gestión de datos hacia otras Entidades del Distrito.

- **Entidades del Grupo B**:
  Deberán consolidar los controles intermedios de seguridad, incluyendo la implementación de Control de Acceso Basado en Roles (RBAC), registros de auditoría sobre sistemas críticos, políticas formalizadas de respaldo y recuperación y mecanismos de gestión y reporte de incidentes alineados con los lineamientos y procedimientos definidos a nivel distrital.

- **Entidades del Grupo C**:
  Deberán priorizar la implementación de los controles mínimos obligatorios del "Mínimo Viable Operativo" (MVO) en materia de seguridad y privacidad, incluyendo:

  1) La publicación y aplicación de la Política de Tratamiento de Datos Personales (Ley 1581 de 2012).
  2) La definición de un protocolo básico de reporte de incidentes.
  3) La restricción del intercambio de bases de datos con información sensible a través de canales no institucionales.
  4) La centralización progresiva de bases de datos en repositorios institucionales oficiales.

  Las Entidades del Grupo C que administren información crítica o soporten la prestación de servicios esenciales para la ciudadanía (como salud, movilidad, hacienda y seguridad) deberán ser objeto de acompañamiento y fortalecimiento priorizado por parte de la Oficina Consejería Distrital de TIC.

Se recomienda que la Oficina Consejería Distrital de TIC defina formalmente:

1) Los criterios de criticidad institucional para la priorización de intervenciones.
2) Los niveles objetivo de madurez en seguridad y privacidad para cada grupo.
3) Los mecanismos de acompañamiento diferenciados para las Entidades del Grupo C.

De la documentación a la acción: materialización en instrumentos de planeación institucional

El diagnóstico de madurez evidencia que múltiples Entidades han desarrollado instrumentos normativos, políticas y procedimientos asociados a seguridad y privacidad de la información. Sin embargo, la existencia de estos documentos formales no garantiza por sí sola la implementación efectiva de los controles ni la generación de valor público a partir de los datos institucionales.

En consecuencia, las recomendaciones contenidas en esta sección deben trascender el plano documental y materializarse en los instrumentos de planeación institucional de cada Entidad, incluyendo:

- Los *Planes Estratégicos de Tecnologías de la Información (PETI),* incorporando las acciones de seguridad y privacidad como componentes obligatorios con indicadores, metas y responsables definidos.

- Los *Planes de Tratamiento de Riesgos de Seguridad y Privacidad de la Información*, asegurando que los controles recomendados se traduzcan en acciones concretas de mitigación con cronogramas y asignación presupuestal.

- Los *Planes de Seguridad de la Información y las Políticas Institucionales*, actualizándolos para reflejar las prioridades derivadas del diagnóstico de madurez y las brechas específicas identificadas en cada Entidad.

Este enfoque orientado a la acción deberá implementarse en el marco del Modelo de Gobernanza de Seguridad Digital definido en el Título 8 del Decreto 640 de 2025, garantizando la articulación entre la gestión de riesgos, los controles de seguridad, los instrumentos de planeación institucional y las instancias de gobernanza establecidas a nivel distrital.

Del cumplimiento normativo al aprovechamiento estratégico de los datos

El diagnóstico de madurez del Distrito evidencia un patrón recurrente según el cual las capacidades asociadas a seguridad digital, privacidad y cumplimiento regulatorio presentan, en términos generales, mayores niveles de desarrollo que aquellas relacionadas con el uso, intercambio y aprovechamiento analítico de los datos para la toma de decisiones.

Este comportamiento sugiere que las Entidades han concentrado sus esfuerzos en la implementación de controles orientados al cumplimiento normativo, mientras que las capacidades necesarias para transformar los datos en información útil para la gestión pública han avanzado a un ritmo menor.

En consecuencia, la implementación del MSPI no debe limitarse a la adopción de controles técnicos y documentales. Por el contrario, debe integrarse de manera explícita con las estrategias de gobierno de datos, calidad de la información, interoperabilidad y aprovechamiento analítico, consolidando una visión en la que la seguridad digital actúe como un habilitador de la gestión basada en datos y no únicamente como un mecanismo de control.

Además, el diagnóstico evidencia que la incorporación de tecnologías no siempre está acompañada de procesos institucionalizados para asegurar la calidad, trazabilidad, administración y aprovechamiento estratégico de la información. Por ello, la seguridad debe concebirse como una capacidad que permite el uso confiable, seguro y sostenible de los datos a lo largo de todo su ciclo de vida.

Avanzar hacia este enfoque integrado resulta fundamental para que el Distrito fortalezca sus capacidades de transformación digital y consolide un modelo de gestión pública donde los datos generen valor para la toma de decisiones, sin comprometer la seguridad, la privacidad ni la confianza ciudadana.

Visión integral (360°) de la gestión de datos y la seguridad digital

Bajo este enfoque, se recomienda que las Entidades adopten una visión integral (360°) de la gestión de datos y la seguridad digital, articulando de manera coordinada la gobernanza del dato, la protección de la información, la gestión de riesgos, el monitoreo continuo y la respuesta ante incidentes.

La implementación del MSPI debe trascender la adopción aislada de controles y evolucionar hacia un modelo de capacidades interrelacionadas que garantice la protección de los activos de información durante todo su ciclo de vida.

En este contexto, las capacidades distritales de monitoreo y respuesta, representadas por la Unidad de Monitoreo de Seguridad Digital (UMSD) y el CSIRT Distrital, constituyen mecanismos de apoyo fundamentales para fortalecer la detección temprana de amenazas, la correlación de eventos de seguridad, la gestión oportuna de incidentes y la resiliencia institucional frente a riesgos que puedan comprometer la confidencialidad, integridad y disponibilidad de la información.

Para materializar esta visión, se formulan las siguientes recomendaciones:

1) **Aprovechamiento de registros de autenticación para el monitoreo distrital**
   Se recomienda habilitar el aprovechamiento de los registros y eventos de autenticación generados por las Entidades, de manera que puedan integrarse progresivamente con las capacidades distritales de monitoreo de seguridad digital. Esto permitirá fortalecer la detección temprana de amenazas, identificar accesos anómalos y generar alertas preventivas orientadas a la protección de los activos de información del Distrito.

2) **Análisis centralizado de eventos de identidad y acceso**
Se recomienda fortalecer las capacidades distritales de detección y respuesta mediante el análisis centralizado de eventos relacionados con identidades y accesos. Este enfoque permitirá identificar oportunamente compromisos de cuentas, elevaciones indebidas de privilegios, accesos atípicos, movimientos laterales y otros comportamientos anómalos que puedan afectar activos de información críticos.

La información analizada deberá integrarse con los mecanismos distritales de monitoreo y gestión de incidentes, promoviendo una visión consolidada de la seguridad digital en las Entidades del Distrito.

3) **Integración de respaldo, recuperación y continuidad operativa con las capacidades de monitoreo**
Se recomienda articular los procesos de respaldo, recuperación y continuidad operativa con los mecanismos institucionales y distritales de monitoreo y gestión de incidentes, permitiendo identificar oportunamente afectaciones sobre información crítica y activar de manera temprana los procedimientos de recuperación.

La integración de estas capacidades fortalece la resiliencia digital de las Entidades, reduce los tiempos de interrupción de los servicios y mejora la capacidad institucional para responder a eventos de ciberseguridad, fallas tecnológicas o incidentes que comprometan la disponibilidad de la información.

4) **Visibilidad y monitoreo de activos de información críticos**
Se recomienda fortalecer la visibilidad sobre los activos de información críticos mediante la integración de inventarios tecnológicos, repositorios de datos y mecanismos de monitoreo de seguridad digital. Esto permitirá mejorar la identificación temprana de activos expuestos, configuraciones inseguras, vulnerabilidades, accesos no autorizados y otros eventos que puedan afectar la confidencialidad, integridad o disponibilidad de la información.

Asimismo, contribuirá a consolidar una visión unificada de los activos digitales del Distrito, facilitando la gestión de riesgos, la priorización de controles y la respuesta oportuna ante incidentes de seguridad.

Complementariamente, se recomienda fortalecer la implementación de los siguientes controles técnicos, organizacionales y operativos alineados con el nivel de criticidad de la información, los riesgos institucionales y las capacidades de madurez identificadas en el diagnóstico:

- **Protección de datos en sus diferentes estados:**
Se recomienda implementar mecanismos de protección sobre la información institucional durante todo su ciclo de uso, incluyendo los datos almacenados, transmitidos y procesados por las Entidades.

  Para ello, las Entidades deben incorporar controles de cifrado (Ej.: AES-256), canales seguros de transmisión (Ej.: protocolos TLS 1.3 o VPN), mecanismos de protección de accesos y medidas de resguardo sobre la información sensible o crítica, priorizando especialmente los datos personales de la ciudadanía y la información estratégica distrital.

  Adicionalmente, se sugiere adoptar estándares técnicos reconocidos internacionalmente para fortalecer la confidencialidad, integridad y disponibilidad de la información institucional.

- **Gestión de identidades y accesos:**
Se recomienda avanzar progresivamente hacia un modelo distrital de gestión de identidades basado en principios de Confianza Cero (Zero Trust), fortaleciendo los mecanismos de autenticación, control de acceso y trazabilidad sobre el uso de la información institucional.

Dado el alto nivel de heterogeneidad tecnológica entre las Entidades distritales, se sugiere implementar un esquema de *Federación de Identidades* que permita mantener la autonomía operativa de cada Entidad, mientras se fortalecen los mecanismos centralizados de autenticación, monitoreo y control de accesos (Ej.: Identity Provider central).

Este enfoque permitiría:

- Fortalecer la adopción de mecanismos de autenticación multifactor (MFA) para usuarios con acceso a información sensible o crítica.
- Mejorar la gestión del ciclo de vida de usuarios (altas, bajas y cambios de rol) y perfiles de acceso, en coordinación con el área de Talento Humano y tecnología de las 63 Entidades.
- Consolidar mecanismos distritales de monitoreo y trazabilidad sobre accesos, autenticaciones y eventos relevantes de seguridad, facilitando la detección temprana de incidentes o comportamientos anómalos. Por ejemplo: recolectar, correlacionar e integrar de forma centralizada en el SOC Distrital los logs de autenticación (sign-in logs y audit logs) de todos los tenants mediante conectores y APIs seguras.
- Favorecer la interoperabilidad segura entre Entidades mediante estándares y mecanismos de autenticación compatibles.

- **Respaldo y recuperación de información:**
  Las Entidades deben fortalecer sus mecanismos de respaldo, recuperación y continuidad operativa sobre la información crítica institucional.

  Para ello, se recomienda implementar políticas de copias de seguridad periódicas, verificadas y protegidas, incluyendo mecanismos de almacenamiento alterno, segmentación de respaldos y esquemas de recuperación ante incidentes de ciberseguridad, fallas operativas o eventos de ransomware.

  Adicionalmente, las Entidades deben validar periódicamente la efectividad de sus procesos de restauración y recuperación, con el fin de asegurar la disponibilidad y continuidad de los servicios críticos.

- **Institucionalización del Ciclo PHVA (Planear, Hacer, Verificar, Actuar):**
  Se recomienda fortalecer la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) mediante la adopción de esquemas de mejora continua basados en el ciclo PHVA, promoviendo la integración entre la gestión de datos, la seguridad digital, la privacidad y la gestión institucional.

  Con este propósito, se sugiere:

  - **Planear:**
    Las Entidades deben fortalecer sus mecanismos de gobernanza para la articulación entre seguridad de la información, privacidad y gestión de datos.

    Para ello, se recomienda formalizar espacios de coordinación institucional, ya sea mediante la creación de un Comité Unificado de Seguridad, Privacidad y Gobierno de Datos o mediante la integración explícita de estas funciones dentro de las instancias ya existentes bajo el marco de MIPG. Este comité estará coliderado por el CIO (o posición similar) y el líder de datos de la Entidad.

    Adicionalmente, se sugiere actualizar las políticas institucionales de seguridad de la información y alinearlas con el Decreto 640 de 2025, reconociendo a la seguridad como un componente transversal del ciclo de vida del dato.

- **Hacer:**
  Implementar progresivamente controles técnicos, operativos y organizacionales orientados a fortalecer la protección de la información institucional, así como desarrollar estrategias permanentes de sensibilización y fortalecimiento de capacidades en seguridad digital y protección de datos.

- **Verificar:**
  Establecer mecanismos periódicos de seguimiento, auditoría y evaluación que permitan medir el nivel de implementación y efectividad de los controles de seguridad, privacidad y gestión de datos, promoviendo espacios de revisión y aprendizaje entre Entidades.

- **Actuar:**
  Definir e implementar planes de mejoramiento continuo que permitan corregir brechas identificadas, fortalecer capacidades institucionales y elevar progresivamente los niveles de madurez en seguridad digital y gestión de datos.

Este enfoque de institucionalización del ciclo PHVA se encuentra alineado con los Lineamientos de Interoperabilidad del Acuerdo 002 de 2025 y los Lineamientos de Inteligencia Artificial del Acuerdo 003 de 2025 de la Comisión Distrital de Transformación Digital (CDTD).

La convergencia entre ambos marcos refuerza la necesidad de que las Entidades adopten el ciclo PHVA como metodología transversal, tanto para la gestión de la seguridad de la información como para el despliegue responsable de tecnologías emergentes, asegurando que la planificación, ejecución, verificación y mejora continua se apliquen de manera integrada a todas las dimensiones de la transformación digital.

- **Inventario y clasificación de activos de información (Art. 214 y 215, Decreto 640 de 2025):** Las Entidades deben mantener inventarios actualizados de sus activos tecnológicos y de información, incluyendo componentes de hardware, software, servicios digitales, repositorios documentales y bases de datos críticas.

  Adicionalmente, se recomienda establecer esquemas de clasificación de la información basados en criterios de confidencialidad, integridad, disponibilidad y criticidad institucional, con el fin de priorizar adecuadamente los controles de seguridad y los mecanismos de protección.

  Asimismo, se sugieren dos acciones específicas:

  1) Incorporar mecanismos de monitoreo y descubrimiento de información que permitan identificar activos, repositorios o conjuntos de datos no registrados formalmente dentro de los inventarios institucionales. Por ejemplo: considerar herramientas de *Data Loss Prevention (DLP)* y escaneo automatizado para descubrir "Shadow Data" (datos no registrados).

  2) Avanzar progresivamente hacia la consolidación de catálogos y esquemas distritales de datos maestros y referenciales, con el fin de fortalecer la consistencia, trazabilidad y confiabilidad de la información estratégica utilizada por las Entidades. Por ejemplo: elaborar un *Catálogo Distrital de Datos Maestros* que defina la única fuente de verdad (Ej.: base de datos de contribuyentes).

- **Priorización de la gestión de datos maestros y referenciales:**
  En atención a la Brecha 1 identificada en el diagnóstico de madurez (gestión de datos maestros y referenciales), considerada una de las principales brechas del ecosistema distrital debido a sus bajos niveles de madurez en los atributos de profundidad, alcance y relevancia, la consolidación de catálogos y esquemas de datos maestros deberá ser priorizada por todas las Entidades del Distrito, independientemente de su grupo de madurez.

El diagnóstico señala que la ausencia de modelos consolidados de datos maestros y referenciales genera duplicidad de información, inconsistencias entre áreas y reprocesos operativos. Como consecuencia, diferentes áreas de una misma Entidad pueden administrar versiones distintas de datos críticos, tales como ciudadanos, proveedores o predios, dificultando la consolidación de una fuente única, confiable y trazable de información institucional.

El alcance de esta acción deberá diferenciarse según el grupo de madurez:

- **Entidades del Grupo C** (rezagadas):
  Deberán iniciar con la identificación y consolidación de los diez (10) activos de datos más críticos de la Entidad, conforme al Mínimo Viable Operativo (MVO) definido en el diagnóstico. Este enfoque gradual permitirá concentrar los esfuerzos institucionales en los activos de información de mayor valor estratégico, facilitando la obtención de resultados tempranos y la expansión progresiva de la estrategia de datos maestros.

- **Entidades del Grupo B** (en transición):
  Deberán avanzar progresivamente hacia una estrategia institucional de gestión de datos maestros que abarque los sistemas misionales prioritarios, estableciendo metas incrementales alineadas con los horizontes definidos en las Hojas de Ruta.

- **Entidades del Grupo A** (líderes):
  Deberán implementar una estrategia integral de datos maestros que cubra la totalidad de los sistemas misionales y asumir un rol activo en la definición de estándares y buenas prácticas transferibles a las demás Entidades.

La Oficina Consejería Distrital de TIC, en coordinación con la Agencia Analítica de Datos, deberá promover la definición de estándares mínimos de metadatos, convenciones de nomenclatura y lineamientos de referencia que faciliten la interoperabilidad entre Entidades, garantizando que las iniciativas institucionales de datos maestros sean compatibles con los esquemas distritales de intercambio y aprovechamiento de información.

- **Controles alineados con estándares internacionales:**
  Se recomienda que las Entidades adopten progresivamente controles alineados con los estándares internacionales de seguridad de la información, como ISO/IEC 27001:2022, priorizando especialmente:

  - **Gestión de accesos y privilegio (A.5.15):**
    Fortalecer los mecanismos de control de acceso para migrar de un modelo de acceso básico a un modelo de *Control de Acceso Basado en Roles (RBAC)* y el *Principio de Menor Privilegio (PoLP)*, asegurando que los usuarios únicamente accedan, con Autenticación Multifactor (MFA), a la información estrictamente necesaria para el desarrollo de sus funciones.

  - **Protección y anonimización de datos sensibles (A.8.11):**
    Implementar mecanismos de anonimización, seudonimización y protección de datos personales, especialmente en ambientes de pruebas, analítica o desarrollo tecnológico, reduciendo la exposición innecesaria de información identificable.

    Se recomienda que los entornos de desarrollo, pruebas o capacitación no utilicen datos reales de ciudadanos sin la aplicación previa de técnicas adecuadas de anonimización, seudonimización o enmascaramiento de datos.

- **Inteligencia de amenazas y monitoreo de seguridad (A.5.7):**
  Fortalecer las capacidades de identificación, análisis y gestión de amenazas de seguridad digital mediante mecanismos de monitoreo continuo, intercambio de información sobre amenazas y generación de alertas tempranas.

  Se recomienda promover la articulación con las capacidades distritales de monitoreo y respuesta para mejorar la detección oportuna de riesgos emergentes, fortalecer la capacidad de respuesta ante incidentes y proteger los activos de información estratégicos del Distrito.

- **Seguridad en el ciclo de desarrollo tecnológico (A.8.25):**
  Incorporar prácticas de seguridad desde las etapas tempranas del desarrollo o adquisición de soluciones tecnológicas, incluyendo validaciones de seguridad, pruebas técnicas y criterios mínimos de protección dentro de los procesos de contratación y desarrollo de software.

  Se sugiere la adopción de la cultura DevSecOps e integrar pruebas de seguridad estáticas (SAST) y dinámicas (DAST) desde la fase de diseño o en los pliegos de contratación tecnológica.

4. MODELO DE GOBERNANZA COMPARTIDA ENTRE GESTIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN

La gestión estratégica de los datos requiere una articulación permanente con las áreas de TI/Sistemas, tales como los responsables de la administración de la información, las áreas de tecnología y seguridad digital, y las instancias encargadas de la privacidad y cumplimiento normativo.

En este contexto, se recomienda fortalecer un modelo de corresponsabilidad institucional que permita integrar las capacidades de gestión de datos, seguridad de la información y protección de datos personales bajo un enfoque coordinado, transversal y alineado con el Decreto 640 de 2025 y el Modelo de Seguridad y Privacidad de la Información (MSPI).

Este enfoque busca asegurar que las decisiones relacionadas con el uso, acceso, protección, intercambio y aprovechamiento de los datos institucionales no se gestionen de manera aislada, sino mediante mecanismos conjuntos de gobernanza, control y gestión del riesgo.

Consideraciones sobre la capacidad institucional y la articulación de roles

Es importante reconocer que las Entidades del Distrito cuentan con capacidades institucionales heterogéneas para implementar los procesos de gobernanza de datos, seguridad de la información y protección de datos personales.

En muchas Entidades, especialmente aquellas con estructuras administrativas más compactas, una misma área o funcionario puede asumir múltiples funciones asociadas a estos ámbitos. Por ejemplo, el Administrador de Datos puede coincidir con el líder de tecnología (CIO), o las responsabilidades relacionadas con privacidad y cumplimiento pueden encontrarse integradas en áreas jurídicas, de planeación o de control interno.

En este contexto, el modelo de gobernanza compartida no debe interpretarse como la necesidad de crear nuevas estructuras organizacionales o cargos especializados, sino como la necesidad de garantizar que las funciones de gestión de datos, seguridad de la información, privacidad, planeación institucional y gestión misional se ejerzan de manera coordinada y complementaria, independientemente de la distribución organizacional adoptada por cada Entidad.

Bajo este enfoque, se recomienda fortalecer mecanismos de articulación que promuevan el trabajo armónico entre el Administrador de Datos, los responsables de seguridad de la información, las áreas de planeación, las dependencias misionales y las áreas administrativas, consolidando un esquema de corresponsabilidad institucional sobre la calidad, protección, disponibilidad y aprovechamiento estratégico de los datos.

Para implementar el modelo de gobernanza compartida, se recomienda:

A. Responsabilidades asociadas a la Gestión de Datos:

- **Clasificación de la información desde el origen:**
  Incorporar criterios de clasificación de la información desde las etapas de captura, creación o diseño de los datos, considerando los lineamientos establecidos en la Ley 1712 de 2014 y la Ley 1581 de 2012, con el fin de facilitar posteriormente la implementación de controles de protección, acceso y tratamiento por parte de las áreas técnicas.

- **Definición de los responsables funcionales del dato:**
  Identificar formalmente a los "Dueños del Dato", que son los responsables funcionales de los datos dentro de las áreas misionales y encargados de definir los criterios de uso, acceso, calidad, conservación y aprovechamiento de la información institucional.

- **Evaluaciones de Impacto en Privacidad (PIA):**
  Promover la realización de evaluaciones de impacto en privacidad (PIA) en iniciativas, proyectos o procesos que involucren el tratamiento de datos personales o información sensible, articulando la participación de las áreas jurídicas, de datos y de tecnología.

B. Responsabilidades asociadas a la Seguridad Digital:

- **Custodia y protección técnica de la información:**
  Implementar los controles tecnológicos y operativos definidos por el MSPI sobre los activos clasificados por el área de datos, necesarios para proteger la información institucional, de acuerdo con su nivel de criticidad, clasificación y sensibilidad e incluyendo mecanismos de control de acceso, cifrado, monitoreo y protección de datos.

- **Trazabilidad y monitoreo de accesos:**
  Fortalecer los mecanismos de monitoreo y auditoría sobre el acceso, consulta, modificación y transferencia de información institucional, promoviendo capacidades de trazabilidad y detección temprana de incidentes o accesos no autorizados.

- **Gestión de riesgos y articulación institucional:**
  Traducir los riesgos técnicos de ciberseguridad y protección de la información en impactos operativos, institucionales y de cumplimiento legal, con el objetivo de facilitar su incorporación dentro de los modelos de gestión de riesgos y toma de decisiones institucionales del marco de MIPG (Ej.: métricas de riesgo del dato)

- **Comités Técnicos de Articulación:**
  Para fortalecer la operativización del modelo de gobernanza compartida y en respuesta a la Brecha 4 del diagnóstico de madurez (limitada madurez en gestión ética y responsable de datos), se recomienda que las Entidades establezcan mecanismos formales de articulación entre las funciones de datos, seguridad, tecnología, privacidad y planeación institucional. Estos mecanismos podrán materializarse mediante un Comité Técnico de Articulación o a través de instancias ya existentes dentro del marco normativo distrital, siempre que se garantice el cumplimiento de las funciones aquí definidas.

Este Comité constituye el vehículo institucional que materializa la gobernanza compartida, evitando que el modelo quede reducido a una declaración de buenas intenciones.

Se sugiere la siguiente composición del Comité:

- Líder de datos o quien ejerza sus funciones.
- Responsable de seguridad de la información (CISO) o quien ejerza sus funciones.
- Líder de tecnología (CIO) o quien ejerza sus funciones.
- Responsable de privacidad y protección de datos personales.
- Un representante del área jurídica o de planeación institucional.

En Entidades donde un mismo funcionario ejerza varios de estos roles, la composición del Comité se adaptará a la estructura organizacional disponible, garantizando como mínimo la participación de las funciones de datos, seguridad y planeación/jurídica.

Las principales funciones del Comité serán:

- Traducir los riesgos técnicos de ciberseguridad en impactos concretos sobre los procesos misionales de la Entidad.
- Revisar y aprobar los casos de uso de datos que requieran controles especiales, tales como el acceso a datos de salud, movilidad o hacienda.
- Evaluar periódicamente el estado de la integración entre la gestión de datos y la seguridad de la información.
- Coordinar la implementación de los lineamientos contenidos en este documento dentro de los instrumentos de planeación institucional (PETI, Planes de Tratamiento de Riesgos y Políticas Institucionales).
- Servir como instancia de enlace con las capacidades distritales de monitoreo (UMSD, CSIRT Distrital) y con el Grupo de Ciberseguridad de la CDTD.

Se sugiere la siguiente frecuencia de sesión diferenciada por grupo de madurez:

- **Entidades del Grupo C** (rezagadas):
  El Comité podrá sesionar con periodicidad bimestral durante los primeros seis (6) meses, focalizando exclusivamente en la implementación del Mínimo Viable Operativo (MVO) y en la articulación de las acciones prioritarias de seguridad y gobernanza de datos.
- **Entidades del Grupo B** (en transición):
  El Comité podrá sesionar con periodicidad trimestral, abordando la consolidación de los controles intermedios y la formalización de los procesos de gobernanza compartida.
- **Entidades del Grupo A** (líderes):
  El Comité podrá sesionar con periodicidad semestral para el seguimiento estratégico y adicionalmente asumir un rol activo de mentoría hacia las Entidades de los Grupos B y C, transfiriendo sus metodologías, políticas, formatos y buenas prácticas institucionales conforme al modelo de "Mentoría Interinstitucional de Datos" recomendado.

C. Inclusión en los planes anuales de auditorías internas:

Para garantizar la efectividad del monitoreo y la trazabilidad de la gobernanza compartida, se recomienda que las Entidades incluyan en sus planes anuales de auditorías internas un componente específico de verificación de la integración entre la gestión de datos y la seguridad de la información.

Este ejercicio deberá tener un enfoque de prevención y autocontrol, orientado a:

- Verificar el funcionamiento efectivo del Comité Técnico de Articulación y el cumplimiento de su periodicidad de sesión.
- Evaluar el grado de materialización de los lineamientos de seguridad y gobernanza de datos en los instrumentos de planeación institucional mencionados (PETI, Planes de Tratamiento de Riesgos y Políticas Institucionales).
- Identificar oportunamente brechas o desviaciones en la implementación de los controles recomendados, antes que se conviertan en hallazgos de auditorías externas o incidentes de seguridad.
- Generar insumos para la mejora continua del modelo de gobernanza compartida en el marco del ciclo PHVA institucional.

La inclusión de este componente en los planes de auditoría interna asegura que el modelo de gobernanza compartida cuente con un mecanismo institucional de verificación y retroalimentación periódica y que los resultados de dicha verificación también alimenten las decisiones del Comité Técnico de Articulación.

5. OPERACIÓN Y GOBERNANZA DE LA GESTIÓN DE INCIDENTES

La consolidación del modelo distrital de seguridad digital requiere fortalecer las capacidades institucionales para la detección, gestión, respuesta y recuperación frente a incidentes que puedan afectar la disponibilidad, integridad o confidencialidad de la información y de los servicios públicos digitales.

En este contexto, la creación y fortalecimiento del CSIRT Distrital, en el marco del Plan Distrital de Desarrollo *"Bogotá Camina Segura"* y del Decreto 640 de 2025, representa un componente estratégico para mejorar la resiliencia digital del Distrito y coordinar la respuesta institucional ante eventos de ciberseguridad.

Adicionalmente, se recomienda que la gestión de incidentes evolucione hacia un enfoque preventivo y basado en inteligencia, integrando capacidades de monitoreo continuo, análisis de amenazas, gestión de vulnerabilidades y protección de activos de información críticos.

Este enfoque permitirá fortalecer la detección temprana de riesgos, anticipar escenarios de afectación sobre los datos y servicios digitales y mejorar la capacidad institucional para tomar decisiones oportunas frente a amenazas emergentes.

La articulación entre la gestión de incidentes, la gestión de riesgos, la gobernanza de datos y las capacidades distritales de monitoreo contribuirá al fortalecimiento de una visión integral de seguridad digital y resiliencia institucional.

Sostenibilidad operativa y mecanismos de financiación

La operación y gobernanza de la gestión de incidentes requiere capacidades organizacionales, tecnológicas y humanas que deben sostenerse en el tiempo. Por lo tanto, la implementación efectiva de los lineamientos contenidos en esta sección depende de que las Entidades incorporen de manera explícita las necesidades de financiamiento, fortalecimiento institucional y desarrollo de capacidades dentro de sus procesos de planeación y gestión presupuestal.

Dado que las Entidades del Distrito presentan niveles heterogéneos de madurez, disponibilidad de recursos y capacidades técnicas, resulta necesario adoptar estrategias diferenciadas que permitan avanzar progresivamente en la implementación de las capacidades de prevención, detección, respuesta y recuperación ante incidentes de seguridad digital.

En consecuencia, se recomienda que cada Entidad, en coordinación con su área de planeación y la Oficina Consejería Distrital de TIC, identifique y articule las fuentes de recursos disponibles para la implementación de las capacidades de gestión de incidentes, considerando las siguientes alternativas:

- **Fichas de inversión institucional:**
  Incorporar los requerimientos de seguridad digital y gestión de incidentes como componentes específicos dentro de los proyectos de inversión registrados en el *Banco Distrital de Programas y Proyectos del Distrito,* mediante sus correspondientes *Fichas de Estadística Básica de Inversión Distrital*, asegurando la definición de indicadores, metas, responsables y asignación presupuestal para su implementación.

- **Recursos propios de funcionamiento:**
  Destinar recursos dentro de los presupuestos de funcionamiento de cada Entidad para la operación sostenida de las capacidades básicas de gestión de incidentes, incluyendo el licenciamiento de herramientas tecnológicas, capacitación del talento humano, actividades de monitoreo y mantenimiento de infraestructura.

- **Cooperación internacional y alianzas estratégicas:**
  Promover la gestión de recursos mediante programas de cooperación internacional, alianzas con organismos multilaterales (BID, CAF, entre otros), acuerdos con el sector privado o programas de fortalecimiento institucional que incluyan componentes de ciberseguridad, protección de datos y transformación digital.

- **Implementación gradual mediante Productos Mínimos Viables (MVP):**
  Adoptar esquemas de implementación gradual basados en Productos Mínimos Viables (MVP), priorizando capacidades esenciales que permitan obtener resultados tempranos, validar los modelos operativos y escalar progresivamente conforme aumenten los niveles de madurez y disponibilidad de recursos.

  Este enfoque resulta particularmente relevante para las Entidades del Grupo C, cuyas restricciones presupuestarias y de capacidad técnica exigen soluciones pragmáticas y de rápida implementación.

La sostenibilidad de las capacidades de gestión de incidentes requiere que las Entidades integren estas necesidades dentro de sus instrumentos de planeación institucional, presupuestal y tecnológica. La identificación temprana de fuentes de financiación y mecanismos de fortalecimiento de capacidades constituye un factor habilitador para la implementación efectiva y progresiva de los lineamientos contenidos en el presente documento.

Para asegurar la efectividad del modelo, se recomienda complementar el enfoque normativo con los siguientes lineamientos operativos, mecanismos de coordinación interinstitucional y procedimientos estandarizados de reporte, escalamiento y atención de incidentes:

- **Modelo operativo distrital de gestión de incidentes:**
  Se recomienda implementar un modelo operativo de cuatro (4) niveles escalonados de gestión de incidentes que permita coordinar de manera articulada las capacidades técnicas, operativas y estratégicas del Distrito:

1) **Nivel Entidad:**
   Responsable de la identificación inicial del evento, aplicación de medidas básicas de contención y activación de los protocolos internos de reporte.

2) **Nivel de monitoreo (SOC Distrital):**
   Encargado del monitoreo continuo, correlación de alertas y generación de capacidades de detección temprana sobre eventos de seguridad digital.

3) **Nivel CSIRT Distrital:**
   Responsable de coordinar técnicamente la atención de incidentes de mayor criticidad, apoyar los procesos de análisis especializado y liderar las acciones de respuesta y recuperación interinstitucional.

4) **Nivel directivo y estratégico:**
   Responsable de la priorización institucional, toma de decisiones estratégicas, gestión reputacional y coordinación de la continuidad operativa frente a incidentes de alto impacto.

Adicionalmente, los diferentes niveles del modelo deberán promover mecanismos permanentes de intercambio de información sobre amenazas, vulnerabilidades, indicadores de compromiso, incidentes y lecciones aprendidas, con el fin de fortalecer la capacidad colectiva de prevención, detección y respuesta de las Entidades Distritales y mejorar la protección de los activos de información estratégicos.

- **Fortalecimiento operativo del CSIRT Distrital (Art. 228.1, Acuerdo 927):**
  Con el propósito de consolidar las capacidades distritales de respuesta ante incidentes de seguridad digital, se recomienda fortalecer progresivamente el modelo operativo del CSIRT Distrital como instancia articuladora de coordinación técnica, monitoreo y respuesta interinstitucional.

  Para este fin, se sugiere considerar los siguientes lineamientos:

  - **Niveles de atención y escalamiento:**
    Definir un esquema progresivo de atención de incidentes que permita clasificar y escalar los eventos según su criticidad, impacto y complejidad técnica. Por ejemplo:
    1) Nivel básico de atención y clasificación inicial del incidente.
    2) Nivel de análisis técnico, contención y mitigación.
    3) Nivel especializado de investigación, coordinación avanzada y recuperación operativa.

  - **Coordinación distrital y articulación nacional:**
    Fortalecer el rol del CSIRT Distrital como punto central de articulación entre las Entidades del Distrito y los organismos nacionales competentes en seguridad digital (Ej.: ColCERT - Grupo de Respuesta a Emergencias Cibernéticas de Colombia), incluyendo mecanismos de coordinación e intercambio de alertas, vulnerabilidades y recomendaciones técnicas.

    Asimismo, se recomienda promover mecanismos formales de intercambio de información de seguridad entre las Entidades Distritales, el CSIRT Distrital, las capacidades de monitoreo de seguridad digital del Distrito y los organismos nacionales competentes, con el propósito de fortalecer la generación de alertas tempranas, compartir lecciones aprendidas y mejorar la capacidad colectiva de prevención y respuesta frente a amenazas comunes.

- **Monitoreo y capacidades de detección:**
  Promover mecanismos de monitoreo continuo y análisis de eventos de seguridad que permitan mejorar la capacidad distrital de identificación temprana de incidentes, comportamientos anómalos y riesgos emergentes.

  Adicionalmente, se recomienda fortalecer las capacidades de inteligencia de amenazas y ciberinteligencia mediante la recolección, análisis e intercambio de información relacionada con amenazas emergentes, vulnerabilidades, indicadores de compromiso (IoC), tácticas, técnicas y procedimientos (TTP) de actores maliciosos.

  Estas capacidades permitirán anticipar riesgos, priorizar acciones preventivas y mejorar la efectividad de los mecanismos de monitoreo, detección y respuesta coordinada frente a incidentes que puedan afectar a las Entidades Distritales.

- **Estandarización operativa:**
  Definir lineamientos comunes de atención, clasificación y escalamiento de incidentes para facilitar la coordinación operativa entre las Entidades distritales y asegurar respuestas homogéneas frente a eventos similares.

- **Protocolos y lineamientos de respuesta a incidentes:**
  Con el objetivo de reducir los tiempos de reacción y fortalecer la capacidad institucional de respuesta, se recomienda establecer protocolos y guías operativas estandarizadas (Playbooks) para la atención de incidentes de seguridad digital.

  Estos lineamientos deben permitir que las Entidades actúen de manera coordinada, documentada y proporcional frente a diferentes escenarios de riesgo.

  Se sugiere considerar los siguientes componentes:

  - **Protocolos estandarizados de atención:**
    Definir procedimientos operativos para la gestión de incidentes asociados a accesos no autorizados, fuga de información, ransomware, indisponibilidad de servicios, pérdida de información o afectaciones sobre infraestructuras tecnológicas críticas.

    Se recomienda incorporar procedimientos específicos para la atención de incidentes asociados a fuga de datos, exposición de información sensible, compromisos de identidad digital, afectaciones a servicios de interoperabilidad y eventos que puedan impactar la confidencialidad, integridad o disponibilidad de los datos utilizados en la operación institucional y en la prestación de servicios a la ciudadanía.

  - **Mecanismos de escalamiento:**
    Establecer criterios claros para determinar cuándo un incidente debe ser escalado a instancias distritales o nacionales, considerando variables como criticidad, impacto institucional, afectación ciudadana o posible compromiso de información sensible.

  - **Lineamientos de contención y recuperación:**
    Definir acciones mínimas para contener incidentes, limitar la propagación de afectaciones, restaurar servicios y asegurar la continuidad operativa de las Entidades.

  - **Actualización y mejora continua:**
    Revisar y actualizar periódicamente los protocolos operativos con base en incidentes reales, lecciones aprendidas, cambios tecnológicos y evolución de las amenazas digitales.

- **Retroalimentación para la gestión de riesgos y protección de datos:**
  Los hallazgos, tendencias, causas raíz y lecciones aprendidas derivadas de los incidentes de seguridad digital deberán incorporarse de manera periódica en los procesos institucionales de gestión de riesgos, protección de datos, continuidad operativa y fortalecimiento de controles.

  Esto permitirá ajustar los mecanismos preventivos, priorizar inversiones de seguridad y mejorar progresivamente la capacidad de las Entidades para anticipar y mitigar riesgos emergentes.

- **Reporte, trazabilidad y gestión de evidencia digital:**
  La gestión adecuada de incidentes requiere fortalecer los mecanismos institucionales de reporte, documentación y trazabilidad de eventos de seguridad digital.

  Por este motivo, se recomienda establecer lineamientos comunes que permitan mejorar la coordinación, el seguimiento y la capacidad de análisis posterior de los incidentes.

  Se sugiere considerar las siguientes recomendaciones:

  - **Canales formales de reporte:**
    Definir mecanismos institucionales para el reporte oportuno de incidentes de seguridad digital (Art. 240, Decreto 640), asegurando que los eventos críticos sean notificados dentro de los tiempos previamente establecidos y siguiendo criterios homogéneos de escalamiento. Por ejemplo, todo incidente crítico debe ser reportado al CSIRT Distrital en un máximo de 4 horas desde su detección (Tiempo de respuesta – SLA).

  - **Trazabilidad operativa:**
    Garantizar el registro y seguimiento de las acciones realizadas durante la atención de incidentes, incluyendo responsables, tiempos de respuesta, medidas de contención y acciones de recuperación implementadas.

  - **Gestión y preservación de evidencia digital:**
    Establecer los lineamientos para la conservación y protección de evidencias digitales asociadas a incidentes de seguridad, garantizando su integridad, autenticidad y disponibilidad para procesos de auditoría, investigación o mejora continua.

  - **Indicadores y seguimiento:**
    Incorporar métricas e indicadores que permitan evaluar los tiempos de atención, tipologías de incidentes, frecuencia, impacto y capacidad de recuperación institucional.

    Asimismo, se recomienda incorporar indicadores orientados a medir la capacidad preventiva y la madurez institucional en materia de seguridad digital, incluyendo métricas relacionadas con detección temprana, tiempos de escalamiento, efectividad de los controles implementados, reincidencia de incidentes, vulnerabilidades recurrentes y nivel de adopción de las acciones de mejora derivadas de eventos anteriores.

- **Cultura institucional y fortalecimiento de capacidades:**
  El fortalecimiento de la seguridad digital no depende exclusivamente de controles tecnológicos, sino también de la capacidad institucional de las Entidades para promover una cultura organizacional orientada a la prevención, protección y uso responsable de la información.

  En este contexto, se recomienda incorporar estrategias permanentes de sensibilización, capacitación y fortalecimiento de capacidades en seguridad digital y protección de datos.

Para este fin, se sugieren las siguientes acciones:

- **Estrategia distrital de concientización en seguridad digital:**
  Diseñar e implementar programas permanentes de sensibilización dirigidos a funcionarios, contratistas y colaboradores sobre buenas prácticas de seguridad digital, manejo seguro de información y prevención de riesgos asociados a ingeniería social, phishing y uso indebido de datos.

  Las estrategias de concientización deberán incorporar escenarios reales observados en las Entidades Distritales, tendencias de amenazas emergentes, casos de fuga de información, campañas de phishing, compromisos de identidad digital y otros eventos relevantes, con el propósito de fortalecer la capacidad de reconocimiento temprano de riesgos y promover una cultura organizacional basada en la prevención y la corresponsabilidad en la protección de la información.

- **Capacitación periódica:**
  Promover procesos de formación continua en temas relacionados con privacidad, protección de datos personales, gestión de incidentes, ciberseguridad y uso seguro de herramientas tecnológicas.

- **Ejercicios de simulación y preparación:**
  Realizar periódicamente ejercicios controlados de simulación de incidentes de seguridad digital para fortalecer la capacidad de respuesta institucional, validar protocolos y generar aprendizaje organizacional. Se sugiere realizar un ejercicio de simulacro distrital anual.

- **Fortalecimiento de capacidades técnicas:**
  Impulsar el desarrollo progresivo de capacidades especializadas en las Entidades distritales para mejorar la gestión de riesgos, monitoreo, respuesta y recuperación frente a incidentes de seguridad digital.

- **Gestión de las Comunicaciones en incidentes de seguridad digital:**
  En concordancia con los objetivos de fortalecimiento de la confianza digital establecidos en la Estrategia Nacional de Seguridad Digital 2025-2027 y alineado con las buenas prácticas internacionales de gestión de incidentes (NIST SP 800-61 y las guías de FIRST), se recomienda incorporar un componente de Gestión de las Comunicaciones dentro de los protocolos de respuesta a incidentes de seguridad digital que afecten servicios públicos digitales o comprometan datos personales, sensibles o estratégicos.

  Los incidentes de seguridad digital pueden trascender el ámbito tecnológico y generar impactos sobre la confianza ciudadana, la continuidad de los servicios, el cumplimiento normativo y la reputación institucional. En consecuencia, las comunicaciones asociadas a la gestión de incidentes deben ser oportunas, consistentes y coordinadas, evitando mensajes contradictorios o la ausencia de información que pueda afectar la confianza digital de la ciudadanía.

  Este componente deberá definir, como mínimo, los siguientes elementos:

  a) Roles y responsabilidades en comunicaciones durante la crisis:

  - Identificación del vocero autorizado de la Entidad para comunicaciones públicas relacionadas con el incidente.

  - Definición de los canales oficiales a través de los cuales se emitirán los comunicados, por ejemplo: portal web institucional, redes sociales institucionales, sala de prensa, aplicativo móvil "Bogotá App", entre otros.

b) Mecanismos de coordinación interinstitucional:

- Establecer protocolos de coordinación entre la Entidad afectada, la Oficina Consejería Distrital de TIC, el CSIRT Distrital y la Alta Consejería Distrital de Comunicaciones, con el fin de asegurar que todos los mensajes emitidos sean consistentes, oportunos y estén libres de contradicciones.

c) Contenidos mínimos de los comunicados de crisis:

- Naturaleza del incidente, sin revelar detalles que comprometan la seguridad o faciliten ataques posteriores.
- Impacto estimado sobre los servicios públicos digitales y los datos de los ciudadanos.
- Medidas adoptadas por la Entidad para contener, mitigar y remediar el incidente.
- Canales de información adicional y puntos de contacto para consultas de la ciudadanía.

d) Oportunidad en las comunicaciones de crisis:

- La Entidad deberá emitir comunicaciones iniciales de manera oportuna, de conformidad con los procedimientos de gestión de incidentes definidos institucionalmente para la atención y coordinación de incidentes de seguridad digital.

e) Protocolos de comunicación posterior al incidente:

- Publicación de informes de lecciones aprendidas y medidas correctivas implementadas, en los plazos que defina el Comité Técnico de Articulación de la Entidad.
- Comunicación proactiva a las partes afectadas sobre las acciones adoptadas para prevenir la recurrencia del incidente.

f) Simulacros sectoriales de comunicación de crisis:

- Las Entidades de los Grupos A y B deberán liderar la realización de simulacros sectoriales de comunicación de crisis al menos una (1) vez al año, incluyendo a Entidades del Grupo C como parte del modelo de mentoría interinstitucional.
- Estos ejercicios de simulación evaluarán la efectividad, claridad y oportunidad de los mecanismos de comunicación definidos y sus resultados alimentarán la mejora continua de los protocolos en el marco del ciclo PHVA.

6. GESTIÓN INTEGRAL DE RIESGOS Y RESILIENCIA DISTRITAL

La gestión de riesgos asociados a la información, los datos y la seguridad digital debe abordarse como un componente transversal de la gestión pública distrital.

En este contexto, se recomienda integrar la gestión de riesgos dentro de los procesos institucionales de planeación, operación, continuidad y toma de decisiones, articulando los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG), el Modelo de Seguridad y Privacidad de la Información (MSPI) y las capacidades de gestión de datos definidas para las Entidades distritales.

El fortalecimiento de la resiliencia digital del Distrito requiere avanzar hacia esquemas coordinados de identificación de riesgos, protección de activos críticos, continuidad operativa y prevención de afectaciones sobre los servicios públicos y la información de los ciudadanos.

Adicionalmente, se recomienda complementar los procesos de gestión de riesgos con capacidades permanentes de monitoreo, análisis de amenazas y evaluación continua de la exposición al riesgo, permitiendo una visión dinámica de los riesgos que afectan a los activos de información, servicios digitales e infraestructuras tecnológicas del Distrito.

Este enfoque favorece la identificación temprana de escenarios emergentes, fortalece la toma de decisiones basada en evidencia y contribuye al incremento progresivo de la resiliencia digital institucional.

Articulación con la Circular 007 de 2024 y reconocimiento de capacidades institucionales

Las acciones de gestión integral de riesgos y resiliencia descritas en esta sección se encuentran alineadas con los lineamientos establecidos en la Circular 007 de 2024, la cual dispone que los Planes Estratégicos de Tecnologías de la Información (PETI) de las Entidades distritales incorporen iniciativas orientadas a la protección de infraestructuras críticas (2.5.1), la gestión de incidentes (2.5.2) y la recuperación ante desastres (2.5.3).

En consecuencia, las recomendaciones aquí formuladas no constituyen obligaciones adicionales, sino que desarrollan y complementan los lineamientos ya establecidos, definiendo criterios y recomendaciones técnicas para facilitar su implementación efectiva.

Las capacidades institucionales, la disponibilidad de recursos y el nivel de madurez de las Entidades del Distrito presentan diferencias significativas. En consecuencia, la implementación de las recomendaciones contenidas en esta sección deberá realizarse bajo un enfoque de proporcionalidad y gestión basada en riesgos, priorizando las acciones de acuerdo con la criticidad de los activos de información, los servicios misionales y el grupo de madurez correspondiente (A, B o C).

Independientemente de lo anterior, todas las Entidades deberán avanzar progresivamente hacia el fortalecimiento de sus capacidades de gestión de riesgos, continuidad operativa y resiliencia digital, procurando alcanzar el mayor nivel de protección posible dentro de sus condiciones institucionales.

Para alcanzar el objetivo de gestión integral y resiliencia distrital, se sugieren las siguientes acciones:

- **Gestión de riesgos y privacidad:**
  Las Entidades distritales deben incorporar la gestión de riesgos asociados a la información, los datos y la seguridad digital dentro de sus procesos institucionales de planeación, operación y control, bajo un enfoque preventivo y basado en riesgos.

  Para este fin, se recomienda adoptar las siguientes metodologías homogéneas de identificación, valoración, tratamiento y monitoreo de riesgos, alineadas con los lineamientos distritales y nacionales vigentes:

  - **Evaluaciones de Impacto en Privacidad (PIA):**
    Implementar los mecanismos de evaluación previa sobre los riesgos asociados al tratamiento de datos personales en proyectos tecnológicos, servicios digitales o iniciativas de interoperabilidad que involucren información de ciudadanos.

  - **Estandarización metodológica:**
    Definir los lineamientos y formatos comunes para la ejecución de evaluaciones de impacto, análisis de riesgos y documentación de controles, con el fin de facilitar criterios homogéneos entre las Entidades distritales.

Por ejemplo: diseñar una plantilla distrital obligatoria de PIA. Ningún proyecto tecnológico nuevo, ya sean aplicaciones móviles, plataformas web ciudadanas u otro, podrá recibir viabilidad presupuestal sin un PIA firmado por el Oficial de Seguridad de la Información (CISO) de la Entidad.

- **Integración con los procesos institucionales:**
  Incorporar los riesgos asociados a los datos, la privacidad y la seguridad digital dentro de los mapas de riesgos institucionales y de los mecanismos de seguimiento definidos en el marco del MIPG.

  Se recomienda que la valoración de riesgos incorpore información proveniente de incidentes de seguridad, vulnerabilidades identificadas, inteligencia de amenazas, hallazgos de monitoreo y tendencias de riesgo observadas a nivel distrital, con el fin de mantener una evaluación actualizada y contextualizada del panorama de amenazas que enfrentan las Entidades.

- **Enfoque preventivo:**
  Promover que las iniciativas tecnológicas y proyectos de transformación digital incorporen criterios de privacidad y seguridad desde las etapas iniciales de diseño y planeación.

- **Infraestructura crítica y activos estratégicos:**
  Se recomienda identificar y priorizar los activos de información, plataformas tecnológicas y servicios digitales cuya afectación pueda impactar la operación institucional, la continuidad de servicios públicos o la toma de decisiones estratégicas del Distrito.

  Para este propósito, las Entidades deberán fortalecer progresivamente sus capacidades de identificación, clasificación y protección de activos críticos.

  Se sugieren las siguientes acciones:

  - **Identificación de activos críticos:**
    Mapear de forma conjunta (Planeación/TI) los sistemas, plataformas y servicios esenciales para la operación distrital, incluyendo aquellos relacionados con movilidad, salud, atención de emergencias, servicios públicos y gestión ciudadana (Ej.: semáforos inteligentes, TransMilenio, Historia Clínica Electrónica Distrital).

  - **Clasificación de información estratégica:**
    Inventariar y clasificar los tableros de control, sistemas analíticos y repositorios de información utilizados para la toma de decisiones estratégicas por parte de la Alta Dirección distrital. De acuerdo con la Ley 1712 de 2014, los tableros se deben catalogar como "Activos de Información Críticos".

  - **Trazabilidad y linaje del dato:**
    Fortalecer la capacidad de identificar el origen, transformación y consumo de la información utilizada en procesos críticos de análisis y toma de decisiones.

    Por ejemplo, el origen de los datos que alimentan los tableros de control. Las áreas de TI deben aplicar de forma obligatoria controles de seguridad específicos sobre este flujo, como el cifrado en tránsito, restricción de acceso por direcciones IP/VPN, enmascaramiento de datos personales de ciudadanos, entre otros.

- **Protección reforzada:**
  Implementar controles diferenciados de acceso, monitoreo y protección sobre los activos clasificados como críticos o estratégicos.

  Asimismo, se recomienda establecer capacidades de monitoreo reforzado sobre los activos críticos y estratégicos, incluyendo mecanismos de detección temprana, supervisión continua de eventos de seguridad y generación de alertas preventivas que permitan reducir la probabilidad de afectaciones significativas sobre la operación institucional y los servicios esenciales para la ciudadanía.

- **Resiliencia y continuidad operativa:**
  La resiliencia digital del Distrito depende de la capacidad institucional para mantener la continuidad de los servicios esenciales y recuperar oportunamente la operación frente a incidentes, fallas tecnológicas o eventos de seguridad digital.

  En este contexto, se recomienda fortalecer las capacidades distritales de continuidad operativa y recuperación tecnológica mediante los siguientes planes, procedimientos y mecanismos de respaldo alineados con la criticidad de los servicios institucionales:

  - **Planes de continuidad y recuperación:**
    Definir y mantener actualizados los Planes de Continuidad de Negocio (BCP) y los Planes de Recuperación ante Desastres (DRP) para los servicios, plataformas y activos de información críticos de cada Entidad. Por ejemplo, para activo y tableros estratégico definir un RTO menor a 2 horas.

  - **Capacidades de recuperación:**
    Establecer objetivos de recuperación acordes con la criticidad institucional de los servicios y fortalecer los mecanismos de respaldo, redundancia y restauración de información.

  - **Pruebas y validación:**
    Realizar ejercicios periódicos de validación y simulación para verificar la efectividad operativa de los planes de continuidad y recuperación.

    Se recomienda complementar estos ejercicios con escenarios de ciberseguridad que involucren ransomware, fuga de información, compromiso de credenciales, indisponibilidad de servicios críticos y afectaciones a infraestructuras tecnológicas estratégicas, permitiendo evaluar de manera integral la capacidad de respuesta y recuperación de las Entidades frente a eventos de alto impacto.

  - **Resiliencia institucional:**
    Fortalecer las capacidades organizacionales que permitan responder, adaptarse y recuperarse de manera coordinada frente a incidentes que afecten la operación institucional o la prestación de servicios al ciudadano.

- **Arquitectura de confianza cero (Zero Trust):**
  Se recomienda avanzar progresivamente hacia esquemas de seguridad basados en el modelo de “Confianza Cero” (Zero Trust), bajo el principio de que ningún usuario, dispositivo o conexión debe considerarse confiable por defecto.

  Este enfoque busca fortalecer la protección de la información mediante mecanismos de validación continua de identidad, control de accesos y monitoreo permanente sobre los activos de información críticos del Distrito.

Para este propósito, se sugieren las siguientes acciones:

- **Validación continua de accesos:**
  Fortalecer los mecanismos de autenticación y control de acceso sobre usuarios, sistemas y servicios críticos, especialmente aquellos que administran información sensible o estratégica. Limitar la confianza basada en la red perimetral.

- **Protección segmentada de entornos críticos:**
  Implementar esquemas de segmentación y protección diferenciada sobre plataformas, redes y repositorios de información de alta criticidad institucional.

- **Verificación contextual de acceso:**
  Incorporar controles que permitan validar continuamente condiciones asociadas a la identidad del usuario, estado de los dispositivos autorizados y contexto de conexión antes de otorgar acceso a información sensible.

- **Reducción de confianza implícita:**
  Reducir progresivamente los modelos tradicionales basados únicamente en acceso a redes internas institucionales, fortaleciendo esquemas de validación permanente y mínimo privilegio.

- **Riesgos de terceros y cadena de suministro:**
  Las Entidades distritales deben fortalecer la gestión de riesgos asociados a proveedores, terceros y servicios tecnológicos contratados, considerando que estos actores también pueden representar vectores de afectación sobre la información, los servicios institucionales y la continuidad operativa.

  En este contexto, se recomienda incorporar criterios mínimos de seguridad digital, continuidad operativa y protección de datos dentro de los procesos de contratación, supervisión y relacionamiento con terceros.

  Se sugieren las siguientes acciones:

  - **Debida diligencia de proveedores:**
    Realizar procesos de evaluación y validación sobre proveedores tecnológicos y servicios críticos, considerando aspectos asociados a seguridad digital, privacidad, continuidad operativa y cumplimiento normativo.

  - **Cláusulas contractuales de seguridad:**
    Incorporar en los contratos y acuerdos de servicio obligaciones relacionadas con seguridad de la información, gestión de incidentes, confidencialidad, respaldo de información y continuidad operativa.

  - **Responsabilidades y mecanismos de reporte:**
    Definir claramente las responsabilidades de terceros frente a incidentes de seguridad digital, así como los mecanismos de notificación, escalamiento y atención coordinada de eventos que puedan afectar la operación institucional.

  - **Monitoreo y evaluación de riesgos:**
    Evaluar periódicamente los riesgos asociados a la cadena de suministro tecnológica y los niveles de exposición institucional derivados de dependencias externas o servicios tercerizados.

    Asimismo, se recomienda incorporar mecanismos de monitoreo y evaluación continua sobre proveedores críticos, servicios en la nube y terceros con acceso a información o infraestructura institucional, permitiendo identificar oportunamente cambios en su nivel de riesgo, vulnerabilidades relevantes o incidentes que puedan generar impactos sobre las Entidades Distritales.

- **Seguridad en los procesos de contratación y gestión de proveedores tecnológicos:** Las Entidades del Distrito deberán incorporar en sus procesos de contratación los lineamientos y cláusulas que permitan garantizar la seguridad de los datos y los activos de información institucional, así como el cumplimiento de los estándares nacionales e internacionales aplicables.

  Este requisito concuerda con los lineamientos de la Circular 007 de 2024 y con las recomendaciones de gobernanza compartida y gestión de riesgos contenidas en el presente documento.

  En este sentido, se sugiere:

  a) Requisito de certificaciones o auditorías independientes para proveedores críticos: Además de las acciones de debida diligencia, cláusulas contractuales y mecanismos de reporte señalados en este documento, se sugiere como requisito que los proveedores de servicios tecnológicos críticos para el Distrito Capital demuestren el cumplimiento de estándares de seguridad reconocidos internacionalmente mediante certificaciones vigentes (Ej.: ISO/IEC 27001, SOC 2, ISO/IEC 27017, ISO/IEC 27018) o, en su defecto, mediante un informe de auditoría independiente que evalúe:

  - Los controles de seguridad aplicables al servicio prestado.
  - El plan de continuidad y recuperación (BCP/DRP) del proveedor.
  - Los registros de incidentes de seguridad de los últimos veinticuatro (24) meses. Esta exigencia es particularmente relevante para:
    - Proveedores que prestan servicios en la nube (IaaS, PaaS, SaaS).
    - Proveedores que administran información clasificada como sensible o estratégica conforme a la Ley 1712 de 2014 y la Ley 1581 de 2012.
    - Proveedores que operan infraestructuras que soportan servicios esenciales para la ciudadanía.

  La exigencia de certificaciones vigentes, estándares reconocidos internacionalmente o informes independientes de auditoría permite evidenciar de manera objetiva la implementación de controles de seguridad por parte del proveedor y facilita los procesos de verificación y debida diligencia de las Entidades.

  Este enfoque se encuentra alineado con los principios de gestión de riesgos, seguridad digital y responsabilidad demostrada promovidos por la Resolución 500 de 2021 del MinTIC y por los lineamientos de protección de datos personales emitidos por la Superintendencia de Industria y Comercio.

  Adicionalmente, los ataques dirigidos a la cadena de suministro tecnológica se han convertido en una de las principales amenazas de ciberseguridad a nivel mundial. En este contexto, las cláusulas contractuales, aunque necesarias, no son suficientes para demostrar que un proveedor ha implementado efectivamente los controles técnicos, organizacionales y operativos requeridos para proteger la información institucional. La verificación independiente de dichas capacidades constituye un mecanismo complementario para fortalecer la gestión del riesgo asociado a terceros.

  b) Acompañamiento diferenciado a Entidades con menores capacidades institucionales: En consideración a las diferencias de madurez, capacidad técnica y disponibilidad de recursos entre las Entidades del Distrito, se recomienda que la Oficina Consejería Distrital de TIC establezca mecanismos de acompañamiento diferenciado para las Entidades del Grupo C, con el fin de fortalecer sus capacidades para la incorporación de requisitos de seguridad de la información en los procesos de adquisición y contratación de bienes y servicios tecnológicos.

Para ello, se sugiere proporcionar:

- Modelos de cláusulas contractuales en materia de seguridad de la información, protección de datos y gestión de incidentes, que puedan ser adaptados e incorporados por las Entidades en sus procesos de contratación

- Listas de verificación y criterios estandarizados de evaluación de seguridad, orientados a facilitar la valoración de proveedores tecnológicos y la identificación de riesgos asociados a terceros.

- Guías y recomendaciones para la verificación de certificaciones, estándares internacionales e informes independientes de auditoría aportados por los proveedores.

Adicionalmente, las Entidades del Grupo A, en el marco del modelo de Mentoría Interinstitucional de Datos, deberán promover la transferencia de conocimiento hacia las Entidades de los Grupos B y C, compartiendo metodologías, matrices de evaluación de proveedores, buenas prácticas y lecciones aprendidas derivadas de sus procesos de contratación y gestión de terceros.

7. INTEROPERABILIDAD SEGURA Y EL TERRITORIO INTELIGENTE

Para consolidar a Bogotá como un “Territorio Inteligente”, el intercambio de información entre Entidades debe realizarse de manera articulada, segura y estandarizada, garantizando simultáneamente la protección de los datos, la trazabilidad de los intercambios y la calidad de la información utilizada para la toma de decisiones públicas.

Además de ser una integración tecnológica, la interoperabilidad distrital debe entenderse como una capacidad institucional que permite compartir datos de forma controlada, confiable y alineada con los principios de gobernanza, seguridad digital y protección de datos personales.

Asimismo, se recomienda que los esquemas de interoperabilidad incorporen capacidades de monitoreo, trazabilidad y gestión de riesgos que permitan supervisar permanentemente los intercambios de información entre Entidades, identificar comportamientos anómalos, detectar accesos indebidos y fortalecer la protección de los datos compartidos.

Este enfoque contribuye a consolidar la confianza digital necesaria para la evolución hacia un “Territorio Inteligente”, seguro, resiliente e interoperable.

Alineación con el esquema de gobernanza de interoperabilidad del Distrito

Las acciones de interoperabilidad segura descritas en esta sección deberán implementarse en el marco del esquema de gobernanza de interoperabilidad contemplado en el Anexo 4 del Acuerdo 002 de 2025 de la CDTD, el cual define la estructura institucional, los roles, las instancias de coordinación y los mecanismos de seguimiento para la gestión de la interoperabilidad a nivel distrital.

Asimismo, la implementación de los lineamientos de interoperabilidad deberá considerar las tres dimensiones establecidas en el Acuerdo 002 de 2025:

- **Dimensión organizacional:** adoptando los acuerdos de confidencialidad e intercambio de información entre Entidades conforme a las plantillas definidas en los Anexos 1 y 2 del Acuerdo.

- **Dimensión técnica:** alineando el diseño de APIs y servicios web con las especificaciones del Anexo 5 y asegurando que los mecanismos de autenticación, autorización, trazabilidad y cifrado cumplan con los estándares de seguridad definidos en el presente documento.

- **Dimensión semántica:** garantizando que los esquemas de datos utilizados en los intercambios de información se alineen con el Estándar de Lenguaje Común de Interoperabilidad promovido por el MinTIC como mecanismo de estandarización semántica para el intercambio de información en el Estado colombiano, en concordancia con el Decreto 1078 de 2015 y los lineamientos de la Comisión Intersectorial de Gobierno Digital.

El rol del Administrador de Datos de cada Entidad, cuyo perfil y responsabilidades se desarrollan en el Anexo 3 del Acuerdo 002, resulta fundamental para la articulación entre las dimensiones de interoperabilidad y los controles de seguridad, asegurando que el intercambio de información se realice bajo estándares de calidad, trazabilidad y protección de datos personales.

Calidad de datos como requisito para la interoperabilidad segura

La interoperabilidad segura requiere que la información intercambiada entre Entidades sea confiable, consistente y apta para su uso. El intercambio de datos inexactos, incompletos, desactualizados o inconsistentes no solo genera ineficiencias operativas y reprocesos institucionales, sino que también incrementa los riesgos asociados a la seguridad de la información, la protección de datos personales y la toma de decisiones basada en datos.

En este contexto, la calidad de los datos debe entenderse como un componente esencial de la interoperabilidad segura y no como una actividad independiente de los procesos de intercambio de información. La confiabilidad de los mecanismos tecnológicos, los controles de seguridad y los esquemas de interoperabilidad depende, en gran medida, de la calidad de los datos que circulan a través de ellos.

En consecuencia, se recomienda que las Entidades incorporen dentro de sus estrategias de interoperabilidad mecanismos de aseguramiento de la calidad de los datos, considerando, como mínimo, las siguientes dimensiones:

- **Exactitud:**
  Los datos intercambiados deben representar de manera correcta y verificable los hechos, eventos o Entidades que pretenden describir. Para ello, las Entidades deberán implementar controles de validación en origen que reduzcan errores de captura, registro y procesamiento de la información.

- **Completitud:**
  Los conjuntos de datos intercambiados deberán contener todos los atributos, campos y registros requeridos conforme a los esquemas de información y Acuerdos de Nivel de Servicio (ANS) definidos entre las partes. La ausencia de información obligatoria deberá ser detectada mediante mecanismos de validación y control que permitan prevenir el intercambio de datos incompletos.

- **Consistencia:**
  Los datos deberán mantener coherencia entre los diferentes sistemas, aplicaciones y repositorios institucionales, así como entre las Entidades que participan en los procesos de interoperabilidad. Las inconsistencias entre fuentes de información afectan la confiabilidad de los datos, dificultan la trazabilidad y pueden generar riesgos operativos, de seguridad y de cumplimiento.

- **Oportunidad:**
  Los datos deberán encontrarse disponibles, actualizados y accesibles en el momento en que sean requeridos para la prestación de servicios, la operación institucional o la toma de decisiones. Los ANS deberán establecer los niveles de servicio esperados en materia de actualización, disponibilidad y tiempos de respuesta para cada flujo de intercambio de información.

- **Uniformidad:**
  Los datos deberán ajustarse a formatos, estructuras, catálogos, nomenclaturas y estándares comunes que faciliten su intercambio, interpretación y reutilización. Para ello, las Entidades deberán alinearse con el Estándar de Lenguaje Común de Interoperabilidad definido por el MinTIC y con los lineamientos técnicos distritales que se adopten para la gestión e intercambio de información.

La adopción de estas dimensiones de calidad deberá realizarse de manera progresiva y proporcional al nivel de madurez de cada Entidad, priorizando en el corto plazo la mejora de la exactitud y completitud de los activos de datos críticos identificados dentro del Mínimo Viable Operativo (MVO), como fundamento para fortalecer la interoperabilidad segura y la confiabilidad de la información a nivel distrital.

Formalización de Acuerdos de Niveles de Servicio – ANS

En atención a la Brecha 3 del diagnóstico de madurez (informalidad en el intercambio de información y acuerdos de niveles de servicio), las Entidades del Distrito deberán priorizar la formalización de Acuerdos de Niveles de Servicio (ANS) para los intercambios de información crítica, estableciendo de manera clara las siguientes condiciones operativas, técnicas, de calidad, seguridad y responsabilidad asociadas a dichos intercambios:

- Responsabilidades y obligaciones de las partes involucradas (Entidad proveedora y Entidad consumidora de información).

- Criterios y niveles mínimos de calidad de los datos intercambiados (exactitud, completitud, consistencia, oportunidad, uniformidad).

- Tiempos de respuesta, disponibilidad y continuidad del servicio de intercambio.

- Mecanismos de trazabilidad, monitoreo y auditoría de las transacciones realizadas.

- Controles de seguridad de la información, privacidad y protección de datos aplicables al flujo de intercambio.

Esto resulta especialmente relevante considerando que el diagnóstico de madurez evidenció que *"la ausencia de acuerdos formales relacionados con tiempos de respuesta, disponibilidad, calidad, trazabilidad y responsabilidades sobre el intercambio de datos limita la consolidación de un ecosistema interoperable, confiable y escalable"*.

Asimismo, el alcance de esta acción deberá diferenciarse según el grupo de madurez:

- **Entidades del Grupo C:**
  Deberán iniciar con la formalización de un (1) ANS para un flujo de intercambio crítico con al menos una Entidad del ecosistema distrital, utilizando los formatos estandarizados (plantillas modelo) definidos en los Anexos 1 y 2 del Acuerdo 002 de 2025 de la CDTD y proporcionados por la Oficina Consejería Distrital de TIC, reduciendo la complejidad y permitiendo un avance gradual.

- **Entidades del Grupo B:**
  Deberán formalizar ANS para los flujos de intercambio de información asociados a sus procesos misionales prioritarios, avanzando progresivamente hacia la formalización de ANS para la totalidad de los intercambios de información considerados críticos para la operación institucional.

- **Entidades del Grupo A:**
  Las Entidades del Grupo A deberán contar con ANS formalizados para la totalidad de sus intercambios de información crítica y promover la exposición de servicios de interoperabilidad seguros, documentados y estandarizados, conforme a los lineamientos establecidos en el Anexo 5 del Acuerdo 002 de 2025, contribuyendo al fortalecimiento del ecosistema distrital de intercambio de información.

La formalización de los ANS constituye un mecanismo fundamental para fortalecer la gobernanza de la interoperabilidad, mejorar la trazabilidad de los intercambios de información y garantizar que los requisitos de calidad, seguridad y disponibilidad de los datos sean gestionados de manera explícita y verificable entre las Entidades participantes.

Complementariamente, para la interoperabilidad segura se sugieren los siguientes lineamientos:

- **Estándares de intercambio e interoperabilidad segura:**
  Las Entidades distritales deben adoptar mecanismos estandarizados de intercambio de información que permitan garantizar la integridad, disponibilidad, confidencialidad y trazabilidad de los datos compartidos entre sectores y plataformas institucionales.

  Se recomienda priorizar arquitecturas interoperables basadas en APIs seguras y servicios estandarizados, incorporando mecanismos de autenticación, autorización y cifrado de extremo a extremo:

  - Implementar arquitecturas de interoperabilidad soportadas en API Gateways y servicios seguros de intercambio de información.

  - Adoptar estándares modernos de autenticación y autorización segura, tales como OAuth 2.0, OpenID Connect o mecanismos equivalentes.

  - Garantizar el cifrado de la información en tránsito mediante protocolos seguros actualizados (Ej.: TLS 1.3).

  - Promover la integración progresiva con los Servicios Ciudadanos Digitales (SCD) y demás plataformas de interoperabilidad definidas por el Gobierno Nacional o el Distrito.

  - Implementar mecanismos de monitoreo y trazabilidad que permitan identificar qué Entidad consume información, cuándo lo hace y en qué condiciones de acceso.

- **Acuerdos de intercambio de información y confidencialidad:**
  El intercambio de información estratégica entre Entidades debe estar soportado mediante instrumentos formales que definan claramente responsabilidades, restricciones de uso, niveles de acceso y obligaciones frente a la protección de datos personales y la seguridad de la información.

  Se recomienda estandarizar modelos distritales de *Acuerdos de Intercambio de Información y Confidencialidad* que faciliten la interoperabilidad institucional bajo criterios homogéneos:

- Formalizar los *Acuerdos de Intercambio de Información y Acuerdos de Confidencialidad* entre las Entidades participantes antes de habilitar mecanismos de interoperabilidad.

- En ambos acuerdos, definir los aspectos relacionados con:
  - Finalidad del intercambio
  - Tipología y clasificación de los datos compartidos
  - Responsabilidades de custodia y tratamiento
  - Restricciones de uso y reutilización
  - Tiempos de conservación
  - Protocolos de notificación ante incidentes
  - Responsabilidad frente a filtraciones o accesos no autorizados

- Estandarizar los formatos distritales de acuerdos para facilitar su adopción transversal entre Entidades.

- **Gobernanza distrital para el intercambio de datos:**
  La interoperabilidad requiere mecanismos de gobernanza que permitan coordinar responsabilidades, priorizar iniciativas estratégicas y asegurar la calidad y trazabilidad de los datos intercambiados.

  En el marco de lo establecido en el Acuerdo 001 de 2025, que adopta el reglamento interno del Comité Distrital de Datos, esta instancia debe consolidarse como el órgano articulador para la definición de los lineamientos, priorización de casos de uso y coordinación institucional alrededor del ecosistema distrital de datos. Además, se sugiere que el Comité asuma las siguientes responsabilidades:

  - Definir y mantener actualizados los roles, responsabilidades y niveles de autoridad asociados a los datos compartidos entre Entidades, diferenciando claramente:
    - Entidad dueña del dato
    - Entidad custodio del dato
    - Entidad consumidora del dato

  - Priorizar los casos de interoperabilidad asociados a servicios críticos para la ciudadanía, analítica distrital y toma de decisiones estratégicas.

  - Garantizar que los intercambios de información cuenten con catálogos de metadatos actualizados, mecanismos de trazabilidad y criterios mínimos de calidad de datos.

  - Promover la adopción de estándares comunes de nomenclatura, estructuras de datos y clasificación de información para reducir inconsistencias entre Entidades.

  - Establecer los mecanismos de seguimiento y monitoreo sobre el uso, disponibilidad y desempeño de los servicios de interoperabilidad distrital.

  La consolidación de un “Territorio Inteligente” requiere que la interoperabilidad se encuentre respaldada por capacidades permanentes de gobernanza, calidad de datos, seguridad digital, protección de datos personales y gestión de riesgos.

  En este contexto, la confianza digital debe constituirse como un principio transversal del ecosistema distrital de datos, garantizando que el intercambio de información genere valor público, fortalezca la toma de decisiones y preserve la seguridad, privacidad e integridad de la información institucional y de la ciudadanía.

8. GESTIÓN RESPONSABLE DE DATOS, TRANSPARENCIA Y TECNOLOGÍAS EMERGENTES

La consolidación de un modelo de "Territorio Inteligente" requiere promover simultáneamente la apertura de la información pública, la protección de los datos personales y el uso responsable de tecnologías emergentes como la analítica avanzada y la inteligencia artificial.

En este contexto, las Entidades distritales deben adoptar un enfoque de **"Seguridad y Privacidad desde el Diseño"**, garantizando que los procesos de publicación, intercambio y aprovechamiento de datos incorporen criterios de transparencia, ética, trazabilidad y protección de derechos desde las etapas iniciales de diseño e implementación.

Complementariamente, se recomienda adoptar un enfoque de confianza digital que integre la gestión de datos, la seguridad de la información, la privacidad y la gestión de riesgos tecnológicos emergentes.

Este enfoque permitirá que la incorporación de nuevas capacidades analíticas, plataformas digitales e iniciativas basadas en inteligencia artificial se desarrollen bajo principios de protección, trazabilidad, transparencia y resiliencia, fortaleciendo la confianza de la ciudadanía en el uso y aprovechamiento de los datos.

La apertura de datos públicos debe realizarse de manera responsable, asegurando mecanismos adecuados de clasificación, anonimización y control de riesgos, especialmente cuando se trate de información sensible o vinculada a ciudadanos.

Adicionalmente, el uso de tecnologías emergentes e inteligencia artificial en procesos institucionales deberá incorporar principios de transparencia, supervisión humana, no discriminación y gestión ética del dato, promoviendo un aprovechamiento seguro y confiable de estas capacidades dentro del ecosistema digital del Distrito.

Clasificación de proyectos de IA y articulación con los grupos de madurez del Distrito

En cumplimiento del Acuerdo 003 de 2025 de la Comisión Distrital de Transformación Digital (CDTD), en concordancia con los lineamientos de la Infraestructura de Datos del Distrito Capital establecidos en el Título 7 del Decreto 640 de 2025 y en armonía con la Política Nacional de Inteligencia Artificial (CONPES 4144 de 2025), las Entidades distritales deberán clasificar sus iniciativas de inteligencia artificial conforme a los niveles de madurez definidos en el Acuerdo (Exploratorio, Consolidación y Avanzado).

Con el fin de promover una adopción responsable, sostenible y acorde con las capacidades institucionales existentes, se recomienda articular dicha clasificación con los grupos de madurez identificados en el diagnóstico distrital de capacidades de datos (Grupos A, B y C).

Esta correspondencia no constituye una restricción para el desarrollo de proyectos de inteligencia artificial, sino una guía para priorizar iniciativas compatibles con el nivel de madurez organizacional, la disponibilidad de datos, las capacidades técnicas y los mecanismos de gobernanza existentes en cada Entidad.

De esta manera, se sugieren las siguientes disposiciones:

Grupo de madurez	Nivel de IA autorizado	Condiciones
Grupo C (rezagadas)	Nivel Exploratorio hasta la consolidación de las capacidades mínimas definidas en el MVO	Las Entidades deberán abstenerse de implementar proyectos de IA que utilicen datos personales reales, tomen decisiones administrativas o afecten derechos de ciudadanos hasta haber consolidado las capacidades fundacionales del MVO.
Grupo B (en transición)	Hasta Nivel Consolidación	Previa evaluación de los impactos sobre la protección de datos personales y la privacidad cuando el tratamiento involucre datos personales, sensibles o decisiones que puedan generar efectos sobre los ciudadanos, conforme al marco normativo vigente en materia de protección de datos personales.
Grupo A (líderes)	Los tres niveles, incluido Nivel Avanzado	Con mecanismos periódicos de evaluación, auditoría y supervisión de los sistemas de IA implementados, así como medidas reforzadas de transparencia y rendición de cuentas conforme al Acuerdo 003 de 2025.

Esta correspondencia progresiva se fundamenta en la conclusión del diagnóstico de madurez según la cual las capacidades avanzadas de analítica e inteligencia artificial requieren como condición habilitante el fortalecimiento previo de las capacidades de gobierno y gestión de datos.

Por ello, las Entidades deberán avanzar gradualmente en la adopción de iniciativas de IA, asegurando que el nivel de complejidad de los proyectos sea consistente con su nivel de madurez institucional y con las capacidades existentes de gobernanza, calidad de datos, seguridad digital, privacidad y gestión de riesgos.

Requisitos mínimos para la contratación de soluciones basadas en Inteligencia Artificial

Además de los requisitos generales de seguridad de la información definidos para los procesos de contratación en la Sección 6 del presente documento, las Entidades que adquieran, desarrollen o implementen soluciones basadas en inteligencia artificial deberán incorporar los siguientes criterios específicos de gobernanza, transparencia, seguridad y trazabilidad que permitan gestionar adecuadamente los riesgos asociados a estas tecnologías:

- **Explicabilidad:**
  El proveedor deberá documentar y comunicar, en términos comprensibles para los usuarios institucionales, los criterios generales de funcionamiento, la lógica, las variables relevantes y las limitaciones conocidas del sistema de IA, permitiendo comprender razonablemente cómo se generan sus resultados, recomendaciones o predicciones.

- **Seguridad de los datos utilizados por el sistema:**
  El proveedor deberá demostrar la existencia de controles orientados a proteger la confidencialidad, integridad y disponibilidad de los datos utilizados para entrenar, validar, ajustar y operar el sistema de IA, incluyendo mecanismos apropiados de anonimización, seudonimización, cifrado y control de accesos cuando corresponda.

- **Trazabilidad:**
  El sistema de IA deberá contar con registros de auditoría que permitan reconstruir las decisiones tomadas, los datos utilizados y las versiones del modelo empleadas en cada momento, conforme a los lineamientos de trazabilidad, supervisión y rendición de cuentas definidos por la normativa distrital aplicable en materia de inteligencia artificial

- **Reporte de incidentes:**
  El proveedor deberá comprometerse a reportar oportunamente incidentes de seguridad, vulnerabilidades identificadas, fallos del modelo, degradación significativa del desempeño, sesgos detectados o cualquier comportamiento anómalo que pueda afectar la confiabilidad, legalidad o seguridad del sistema de IA, conforme a los protocolos institucionales y distritales de gestión de incidentes.

- **Supervisión humana:**
  Las soluciones de IA que apoyen procesos misionales, decisiones administrativas o servicios dirigidos a la ciudadanía deberán incorporar mecanismos que permitan la revisión, validación o intervención humana cuando la naturaleza del proceso, el nivel de riesgo o el impacto potencial sobre los ciudadanos así lo requieran.

Gobernanza institucional de la IA

El Comité Distrital de Datos, reglamentado por el Acuerdo 001 de 2025 del Comité Distrital de Datos, deberá actuar como instancia de articulación, seguimiento y coordinación estratégica para la implementación de la Estrategia Distrital de Datos e Inteligencia Artificial, promoviendo la alineación entre las iniciativas institucionales, los lineamientos distritales y los mecanismos de gobernanza definidos para el ecosistema de datos del Distrito.

En este marco, se recomienda que el Comité impulse las siguientes acciones:

- Validar la clasificación de los proyectos de IA conforme a los niveles de madurez definidos por la normativa distrital.

- Formular recomendaciones sobre los proyectos de Nivel Avanzado que involucren datos personales o puedan incidir en decisiones administrativas, de acuerdo con las competencias que le sean asignadas por la normativa vigente.

- Dar seguimiento a los resultados de las auditorías algorítmicas realizadas por las Entidades del Grupo A, promoviendo la adopción de acciones de mejora, la mitigación de riesgos identificados y la transferencia de buenas prácticas hacia las demás Entidades del Distrito.

- Articular con el Grupo de Ciberseguridad de la CDTD la identificación, evaluación y tratamiento de los riesgos de seguridad digital asociados a los sistemas de inteligencia artificial implementados por las Entidades distritales.

Complementariamente, se sugieren los siguientes lineamientos:

- **Transparencia y apertura responsable de datos:**
  El fortalecimiento de la transparencia institucional y del modelo de Gobierno Abierto requiere promover el acceso y reutilización de la información pública, garantizando simultáneamente la protección de los datos personales y la seguridad de la información.

  En este contexto, las Entidades distritales deben adoptar el principio de **“Abierto por Defecto”**, según el cual la información pública debe estar disponible para consulta y reutilización ciudadana, salvo en aquellos casos donde existan restricciones legales asociadas a privacidad, reserva o seguridad pública.

Con este fin, se recomienda:

- Promover la publicación progresiva de conjuntos de datos abiertos de alto valor para la ciudadanía, analítica distrital y control social.

- Clasificar la información institucional conforme a los criterios establecidos en la Ley 1712 de 2014 y la Ley 1581 de 2012, diferenciando información pública, clasificada y reservada.
- Mantener actualizado y publicado el Índice de Información Clasificada y Reservada (IICR) de cada Entidad.

- Implementar mecanismos de validación y control previo a la publicación de datasets abiertos, verificando calidad, integridad y consistencia de la información.

- Promover esquemas de trazabilidad y documentación de metadatos para facilitar la reutilización e interpretación de la información publicada.

- **Protección de datos personales y desidentificación de información:**
  La apertura e intercambio de información pública debe realizarse bajo criterios de privacidad desde el diseño, minimización de datos y protección de los derechos de los titulares de la información.

  Antes de publicar, compartir o utilizar conjuntos de datos con fines analíticos o de interoperabilidad, las Entidades deben aplicar los siguientes mecanismos técnicos y organizacionales orientados a reducir el riesgo de identificación directa o indirecta de personas:

  - Implementar los mecanismos de anonimización, seudonimización, enmascaramiento o desidentificación de información sensible antes de publicar o intercambiar datos.

  - Evitar la exposición de datos personales, sensibles o reservados en portales de datos abiertos, tableros públicos o ambientes de pruebas.

  - Establecer los procedimientos de revisión y validación de privacidad previos a la publicación de información institucional.

  - Aplicar los principios de minimización y proporcionalidad en el tratamiento de datos personales utilizados para procesos analíticos o estadísticos.

  - Promover la incorporación de criterios de privacidad desde el diseño en nuevos sistemas de información, plataformas digitales y procesos de interoperabilidad.

  Se recomienda complementar estos mecanismos con evaluaciones periódicas de su efectividad, con el fin de verificar que las técnicas de anonimización y desidentificación continúen siendo adecuadas frente a la evolución de las capacidades tecnológicas y a los riesgos de correlación o reidentificación derivados de la integración de datos provenientes de múltiples fuentes de información.

- **Uso responsable de tecnologías emergentes e inteligencia artificial**
  El aprovechamiento de tecnologías emergentes, analítica avanzada e inteligencia artificial representa una oportunidad para fortalecer la eficiencia institucional y la toma de decisiones basada en datos.

  Sin embargo, su implementación debe realizarse bajo principios de transparencia, ética, supervisión humana y protección de derechos, especialmente cuando dichas tecnologías puedan generar impactos sobre los ciudadanos o poblaciones vulnerables.

Con este fin, se recomienda:

- Promover la adopción de principios éticos para el desarrollo y uso de modelos analíticos e inteligencia artificial dentro de las Entidades distritales.
- Implementar mecanismos de evaluación y revisión de modelos analíticos para identificar posibles sesgos, riesgos de discriminación o afectaciones sobre grupos poblacionales vulnerables.
- Garantizar los criterios mínimos de transparencia, trazabilidad y explicabilidad sobre los resultados generados por sistemas automatizados de decisión.
- Promover los esquemas de supervisión humana en procesos críticos soportados por inteligencia artificial o analítica predictiva.
- Evaluar la viabilidad de implementar espacios controlados de experimentación ("Sandboxes") que permitan probar tecnologías emergentes bajo lineamientos técnicos, éticos y regulatorios definidos por el Distrito.
- Establecer lineamientos específicos para el uso responsable de inteligencia artificial en procesos relacionados con servicios ciudadanos, asignación de beneficios, analítica de seguridad, inspección, vigilancia y control, entre otros casos de alto impacto público.

- **Gobernanza y supervisión del uso de tecnologías emergentes y datos:**
  La incorporación de nuevas capacidades analíticas y tecnológicas requiere fortalecer los mecanismos institucionales de gobernanza, seguimiento y control sobre el uso de los datos.

  Por esta razón, las Entidades deben garantizar que los procesos de innovación tecnológica se encuentren alineados con los lineamientos distritales de gestión de datos, seguridad digital, privacidad y gestión de riesgos.

  Con este fin, se recomienda:

  - Incorporar criterios de evaluación ética, privacidad y seguridad dentro de los procesos de adquisición o contratación de soluciones basadas en inteligencia artificial o analítica avanzada.
  - Definir los responsables institucionales para supervisar el uso de datos y tecnologías emergentes en procesos estratégicos de la Entidad.
  - Articular las iniciativas de innovación tecnológica con los esquemas institucionales de gestión de riesgos, continuidad operativa y seguridad digital.
  - Promover los mecanismos de monitoreo y revisión periódica sobre el desempeño, riesgos y resultados de las soluciones analíticas implementadas.

9.CONCLUSIONES ESTRATÉGICAS DE ALINEACIÓN INSTITUCIONAL

La consolidación de un modelo distrital de gestión de datos, seguridad digital y privacidad requiere avanzar hacia esquemas de gobernanza articulados, sostenibles y con responsabilidades claramente definidas entre las áreas misionales, tecnológicas y de planeación institucional.

Para lograrlo, las Entidades distritales deberán fortalecer progresivamente sus capacidades institucionales en materia de gestión de riesgos, protección de la información, interoperabilidad segura y monitoreo operativo, asegurando la alineación entre los lineamientos de gestión de datos y los controles de seguridad digital definidos a nivel distrital y nacional.

Enfoque diferenciado y proporcional basado en el diagnóstico de madurez

Con base en los resultados del Instrumento de Madurez de Capacidades (IMC) y los ejercicios de evaluación realizados en las Entidades distritales, se evidencia que el ecosistema institucional presenta niveles heterogéneos de desarrollo en materia de gestión de datos, seguridad digital y privacidad. En este contexto, las Entidades pueden agruparse en tres categorías operativas:

- **Grupo A** (líderes y pioneros): Entidades con capacidades institucionalizadas y sostenibles.
- **Grupo B** (instituciones en transición): Entidades con capacidades emergentes y procesos en consolidación.
- **Grupo C** (rezagados críticos): Entidades con niveles incipientes de institucionalización y mayores brechas de capacidad.

En consecuencia, las estrategias de fortalecimiento en materia de seguridad digital, privacidad y gobernanza de datos deberán implementarse bajo un enfoque diferenciado y proporcional al nivel de madurez de cada Entidad, priorizando las acciones de acuerdo con sus capacidades institucionales, la criticidad de los activos de información y los riesgos asociados a sus procesos misionales.

Este enfoque se encuentra alineado con el principio de proporcionalidad promovido por el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, con el enfoque basado en riesgos establecido por la norma ISO/IEC 27001:2022 y en articulación con los resultados de la categoría de Seguridad y Privacidad del Instrumento de Madurez de Capacidades (IMC) y los ejercicios de diagnóstico de ciberseguridad realizados en 2025.

Mínimo Viable Operativo (MVO) como línea base transversal

Todas las Entidades del Distrito, independientemente de su grupo de madurez, deberán garantizar la implementación y sostenibilidad del Mínimo Viable Operativo (MVO) como línea base transversal obligatoria para la gestión de datos, la seguridad digital y la privacidad de la información. El MVO comprende los siguientes diez (10) componentes fundacionales:

1. **Nombrar oficialmente al Administrador de Datos**, conforme al perfil definido en el Anexo 3 del Acuerdo 002 de 2025 de la CDTD.
2. **Articular la función de gobierno de datos a través del Comité Institucional de Gestión y Desempeño (CIGD)** de la Entidad, como instancia interna de coordinación entre las funciones de gestión de datos, seguridad digital, planeación institucional y áreas misionales.

3. **Crear y mantener un inventario de los activos de datos más críticos** de la Entidad, identificando su ubicación, custodio, nivel de clasificación y sistemas de información asociados.

4. **Definir un Diccionario de datos básico** que documente la estructura, definiciones y relaciones de los activos de datos críticos inventariados.

5. **Publicar y aplicar la Política de Tratamiento de Datos Personales** conforme a la Ley 1581 de 2012 y sus decretos reglamentarios.

6. **Definir un protocolo básico de reporte de incidentes** de seguridad digital y privacidad de la información, alineado con los procedimientos del CSIRT Distrital.

7. **Mapear y cruzar los activos críticos con la Tabla de Retención Documental (TRD)**, garantizando la articulación entre la gestión documental y la gestión de datos.

8. **Documentar el flujo de los activos de datos críticos**, describiendo su origen, transformaciones, destinos y controles de seguridad aplicables en cada etapa.

9. **Adoptar lineamientos para el uso de formatos estándar** (CSV, JSON, XML) en el reporte oficial de datos, facilitando la interoperabilidad y el aprovechamiento analítico de los datos.

10. **Incorporar iniciativas de gestión de datos en la planeación institucional**, garantizando que la Entidad contemple en el presupuesto los recursos para al menos una (1) iniciativa orientada a fortalecer sus capacidades de datos.

El cumplimiento del MVO constituye la condición habilitante para el desarrollo progresivo de capacidades avanzadas en materia de seguridad digital, interoperabilidad, analítica e inteligencia artificial. En consecuencia, las Entidades deberán priorizar el cierre de las brechas asociadas a estos componentes fundacionales antes de emprender iniciativas de mayor complejidad tecnológica o analítica.

Prioridades diferenciadas por grupo de madurez

Más allá del cumplimiento del Mínimo Viable Operativo (MVO), cada grupo de madurez deberá orientar sus esfuerzos hacia prioridades específicas de fortalecimiento, de acuerdo con sus capacidades institucionales, las brechas identificadas en el diagnóstico y los objetivos de evolución definidos para cada nivel.

Grupo C: Ordenamiento operativo y cumplimiento básico

Las Entidades del Grupo C deberán concentrar sus esfuerzos en el ordenamiento operativo y el cumplimiento de los controles mínimos, con énfasis en:

- **Centralizar las bases de datos** en repositorios institucionales oficiales, reduciendo progresivamente la dispersión de información en hojas de cálculo, correos electrónicos y dispositivos personales.

- **Definir controles básicos de validación desde el punto de captura de la información**, implementando reglas básicas de calidad que eviten el ingreso de datos incompletos, duplicados o inconsistentes en los sistemas de información.

- **Restringir el intercambio de información sensible** por canales no autorizados o no institucionalizados (Ej.: correo personal, aplicaciones de mensajería o dispositivos USB no institucionales).

- **Adoptar convenciones estandarizadas de nomenclatura documental**, alineadas con las directrices de la Oficina Consejería Distrital de TIC y la Agencia Analítica de Datos.

- **Definir el ciclo de vida de los datos,** estableciendo los criterios básicos de almacenamiento, conservación y depuración de la información y los lineamientos para la eliminación controlada de registros temporales, duplicados o sin valor operativo.

Grupo B: Consolidación de estándares, integración e incorporación de automatización

Las Entidades del Grupo B deberán avanzar hacia la consolidación de estándares y la integración de información, con énfasis en:

- **Implementar un esquema formal de administración y custodia de datos** por sistema de información, definiendo para cada uno el administrador de datos de la Entidad, el responsable funcional de datos (dueño del dato) y el custodio técnico de datos correspondiente.

- **Identificar y consolidar los datos maestros y referenciales críticos**, avanzando progresivamente hacia estrategias institucionales que abarquen los sistemas misionales prioritarios.

- **Implementar el Control de Acceso Basado en Roles (RBAC) y registros de auditoría** sobre los sistemas de información que gestionan datos críticos o sensibles.

- **Capturar los metadatos mínimos para documentos electrónicos**, asegurando la trazabilidad, clasificación y recuperabilidad de la información institucional.

- **Definir el ciclo de vida de los datos,** estableciendo las políticas de respaldo, conservación, archivo histórico y eliminación segura de la información, así como alinear las políticas con los tiempos de retención establecidos en las Tablas de Retención Documental (TRD) y con los lineamientos de seguridad y gestión documental de la Entidad.

- **Formalizar al menos un (1) Acuerdo de Nivel de Servicio (ANS)** para el intercambio de información con otra Entidad, conforme a las plantillas definidas en los Anexos 1 y 2 del Acuerdo 002 de 2025 de la CDTD.

Grupo A: Innovación pública basada en datos, analítica avanzada y liderazgo institucional

Las Entidades del Grupo A, además de mantener y profundizar los estándares alcanzados, deberán asumir un rol de liderazgo e innovación, con énfasis en:

- **Adoptar el modelo de Mentoría Interinstitucional de Datos** para acompañar activamente a Entidades de menor madurez, transfiriendo metodologías, políticas, formatos y buenas prácticas.

- **Evolucionar hacia catálogos de datos automatizados**, que permitan la actualización dinámica del inventario de activos de datos y la generación automática de metadatos.

- **Implementar mecanismos de anonimización y seudonimización** para información sensible, habilitando el aprovechamiento analítico de datos sin comprometer la privacidad.

- **Integrar los Sistemas de Gestión de Documentos Electrónicos de Archivo (SGDEA) y los repositorios de datos estructurados**, contribuyendo a superar la desarticulación entre la gestión documental y la gestión de datos identificada en la Brecha 2 del diagnóstico.

- **Definir el ciclo de vida de los datos,** implementando estrategias de automatización de gestión y optimización del almacenamiento de información y estrategias de optimización de recursos tecnológicos y presupuestales de la Entidad.

- **Exponer los servicios de interoperabilidad seguros (APIs documentadas)** conforme al Anexo 5 del Acuerdo 002 de 2025, contribuyendo al Catálogo Distrital de Servicios de Interoperabilidad.

La transición entre grupos de madurez no deberá entenderse como una sustitución de capacidades, sino como un proceso acumulativo. En consecuencia, las Entidades deberán mantener los controles y prácticas correspondientes a los niveles anteriores mientras avanzan hacia capacidades de mayor complejidad y sofisticación.

Inteligencia Artificial: restricciones y habilitaciones según el grupo de madurez

En materia de inteligencia artificial, las Entidades deberán clasificar sus iniciativas conforme a los niveles de madurez definidos en el Acuerdo 003 de 2025 de la CDTD (Exploratorio, Consolidación y Avanzado), aplicando las restricciones, condiciones y habilitaciones correspondientes a su grupo de madurez institucional, de acuerdo con lo establecido en la Sección 8 del presente documento.

De esta manera, se reconoce que el aprovechamiento seguro, ético y efectivo de la inteligencia artificial depende del fortalecimiento previo de las capacidades de gestión de datos, calidad de información, gobernanza, seguridad digital y protección de datos personales.

En consecuencia, la evolución hacia los casos de uso de mayor complejidad deberá realizarse de manera progresiva y proporcional al nivel de madurez alcanzado por cada Entidad.

Bajo este enfoque, las Entidades del Grupo C deberán concentrarse inicialmente en los casos de uso exploratorios y de bajo riesgo; las Entidades del Grupo B podrán avanzar hacia escenarios de consolidación una vez fortalecidas sus capacidades de gobierno y protección de datos; y las Entidades del Grupo A estarán capacitadas para desarrollar iniciativas avanzadas de inteligencia artificial, acompañadas de mecanismos reforzados de transparencia, auditoría, supervisión humana y gestión de riesgos.

Tabla de roles y responsabilidades diferenciada

La implementación de los roles y responsabilidades definidos en el presente documento deberá realizarse de manera proporcional al nivel de madurez de cada Entidad, reconociendo que las capacidades institucionales, la disponibilidad de recursos y las estructuras organizacionales son heterogéneas en el Distrito.

En consecuencia, las Entidades de menor madurez podrán asignar múltiples funciones a una misma persona o equipo de trabajo, siempre que se garantice el cumplimiento efectivo de las responsabilidades asociadas a la gestión de datos, la seguridad digital, la privacidad y la gestión de riesgos.

Por su parte, las Entidades del Grupo A deberán avanzar progresivamente hacia la especialización, formalización y segregación de funciones, fortaleciendo los mecanismos de gobernanza y control institucional.

Con el fin de facilitar la implementación homogénea de estos lineamientos, se recomienda que la Oficina Consejería Distrital de TIC evalúe la elaboración de un instrumento operativo complementario que detalle, para cada grupo de madurez (A, B y C):

- Los roles mínimos recomendados y su alcance funcional.
- Los entregables y evidencias esperadas para cada horizonte de implementación de las Hojas de Ruta.
- Los indicadores de seguimiento y los criterios orientadores para la evolución de capacidades institucionales de un grupo a otro.
- Las plantillas, formatos, guías y herramientas de referencia que faciliten la adopción de los lineamientos por parte de las Entidades con menores capacidades institucionales.

Este instrumento permitiría traducir los lineamientos estratégicos del presente documento en orientaciones operativas diferenciadas, facilitando una implementación gradual, consistente y alineada con las capacidades reales de las Entidades del Distrito.

De igual forma, será fundamental consolidar los mecanismos de coordinación con el SOC Distrital, el CSIRT Distrital y las instancias institucionales de gobernanza, promoviendo una visión integrada de seguridad, privacidad y aprovechamiento estratégico de los datos dentro del ecosistema digital de Bogotá.

Adicionalmente, se recomienda consolidar una visión integral (360°) de la gestión de datos y la seguridad digital, en la cual la gobernanza de datos, la protección de la información, la gestión de riesgos, el monitoreo continuo, la inteligencia de amenazas, la respuesta a incidentes y la resiliencia operativa funcionen como capacidades complementarias y articuladas.

Este enfoque permitirá fortalecer la confianza digital, mejorar la toma de decisiones basada en datos y garantizar que la transformación digital del Distrito se desarrolle bajo principios de seguridad, privacidad, transparencia y sostenibilidad institucional.

La implementación de estos lineamientos permitirá fortalecer la resiliencia institucional, mejorar la capacidad de respuesta ante incidentes y consolidar las bases necesarias para avanzar hacia un modelo de “Territorio Inteligente” más confiable, interoperable y centrado en la ciudadanía.

La siguiente tabla resume los principales roles y responsabilidades asociados a la articulación entre gestión de datos, seguridad digital y gobernanza institucional:

Componente	Gestión de Datos	Seguridad Digital / TI	Gobernanza Integrada
Enfoque principal	Clasificación, definición de uso y criticidad de los activos de información conforme a la normativa vigente (Ley 1712 y 1581).	Implementación de controles técnicos, protección de infraestructuras y aplicación del MSPI (ISO 27001).	Articulación institucional mediante Comités y esquemas integrados de seguridad, privacidad y datos.
Identidad y acceso	Definición de perfiles autorizados y responsables funcionales del acceso a la información	Gestión de identidades, autenticación multifactor, trazabilidad y monitoreo de acceso.	Coordinación institucional para garantizar control, trazabilidad y administración segura del ciclo de vida de usuarios y accesos.
Activos críticos	Identificación de datos estratégicos, tableros críticos y trazabilidad de la información (linaje).	Monitoreo continuo de la infraestructura crítica, incidentes y eventos de seguridad digital, mediante el SOC y CSIRT Distrital.	Seguimiento integral y reporte articulado MIPG para la ampliación de la cobertura a las 63 Entidades.

10. HOJA DE RUTA ESTRATÉGICA PARA LA IMPLEMENTACIÓN

Con el propósito de facilitar la implementación progresiva de los lineamientos propuestos en este documento, se recomienda estructurar una hoja de ruta distrital basada en horizontes de corto, mediano y largo plazo.

Este enfoque permite priorizar acciones de impacto inmediato, consolidar capacidades institucionales y evolucionar progresivamente hacia un modelo distrital integrado de gestión de datos, seguridad digital e interoperabilidad segura.

La implementación deberá combinar componentes de gobernanza, fortalecimiento institucional, capacidades operativas, gestión de riesgos y modernización tecnológica, bajo un enfoque gradual y proporcional a las capacidades de cada Entidad.

Para alcanzar los objetivos propuestos, sugerimos:

Fase	Plazo	Prioridades Estratégicas	Resultados Esperados
Corto plazo	0 - 6 meses	Formalización de la gobernanza, identificación de activos críticos, fortalecimiento de controles mínimos obligatorios y definición de lineamientos de seguridad y privacidad	Reducción de riesgos prioritarios, fortalecimiento institucional inicial y mayor visibilidad sobre los activos críticos de las 63 Entidades
Mediano plazo	6 - 12 meses	Consolidación operativa del modelo distrital de seguridad y gestión de datos mediante el fortalecimiento de capacidades técnicas, monitoreo coordinado, protección de información sensible y estandarización de procesos institucionales.	Mayor capacidad de prevención, detección y respuesta frente a incidentes y fortalecimiento de la gestión y protección de los datos institucionales.
Largo plazo	12 - 24 meses	Evolución hacia un ecosistema distrital interoperable, resiliente y basado en principios de confianza digital, analítica avanzada y automatización segura de procesos	Consolidación de un modelo distrital con capacidades sostenibles de interoperabilidad, ética, resiliencia operativa y aprovechamiento estratégico de los datos.

Hoja de Ruta diferenciada por grupo de madurez

Con base en los hallazgos del diagnóstico de madurez y en el modelo de Mentoría Interinstitucional de Datos, la implementación de la Hoja de Ruta deberá considerar enfoques diferenciados según el grupo de madurez de cada Entidad, respetando las capacidades reales y evitando exigencias desproporcionadas que generen frustración operativa.

La presente propuesta deberá validarse con los avances y acciones que viene realizando el equipo de Ciberseguridad del Distrito, asegurando la complementariedad y evitando la duplicación de esfuerzos.

Corto plazo (0–6 meses)

Entidades del Grupo C:

- Implementar prioritariamente el Mínimo Viable Operativo (MVO) sugerido:
  - Administrador de Datos
  - Asignación de gobierno de datos al Comité Institucional de Gestión y Desempeño (CIGD)

- Inventario de los diez (10) activos de datos más críticos
- Diccionario de datos básico
- Publicación de la Política de Tratamiento de Datos Personales
- Protocolo básico de reporte de incidentes
- Mapeo de activos críticos con la TRD
- Documentación del flujo de los activos críticos
- Adopción de formatos estándar (CSV, JSON, XML)
- Incorporar iniciativas de datos en instrumentos de planeación institucional y presupuestal

Entidades del Grupo B:

- Consolidar los roles de gobierno y custodia de datos en los sistemas de información críticos.
- Implementar el Control de Acceso Basado en Roles (RBAC) y registros de auditoría sobre sistemas de información críticos.
- Iniciar la consolidación de datos maestros y referenciales en procesos misionales prioritarios.
- Capturar metadatos mínimos para documentos electrónicos.
- Formalizar al menos un (1) Acuerdo de Nivel de Servicio (ANS) para intercambio de información conforme a las plantillas del Acuerdo 002 de 2025.

Entidades del Grupo A:

- Preparar los "Kits de Aceleración": documentar políticas, formatos, plantillas y metodologías propias en paquetes estandarizados transferibles a las Entidades Acompañadas.
- Identificar las Entidades de los Grupos B y C que serán acompañadas mediante el modelo de Mentoría Interinstitucional de Datos, en coordinación con la Oficina Consejería Distrital de TIC.
- Iniciar la automatización de los catálogos de datos, exponer estándares de interoperabilidad y capacidades avanzadas de monitoreo y analítica.

Mediano plazo (6–12 meses)

Entidades del Grupo C:

- Implementar controles básicos de calidad de datos mediante la centralización de bases de datos en repositorios institucionales oficiales.
- Implementar mecanismos de validación en el punto de captura para activos de datos críticos.
- Restringir el intercambio de información sensible por canales no autorizados.
- Adoptar convenciones estandarizadas de nomenclatura documental.

Entidades del Grupo B:

- Implementar interoperabilidad automatizada: consumo de al menos un (1) servicio externo mediante API o Web Service conforme al Anexo 5 del Acuerdo 002 de 2025.
- Formalizar e implementar una estrategia institucional de datos maestros y referenciales para los activos críticos de los sistemas misionales prioritarios.
- Alinear políticas de respaldo y recuperación con la Tabla de Retención Documental (TRD).

Entidades del Grupo A:

- Implementar el modelo de Mentoría Interinstitucional de Datos, acompañando a las Entidades asignadas mediante sesiones periódicas de transferencia de conocimiento.
- Transferir los "Kits de Aceleración" y apoyar su adopción en las Entidades Acompañadas.
- Documentar y compartir buenas prácticas, lecciones aprendidas y casos de éxito derivados de los procesos de mentoría.
- Implementar capacidades avanzadas de anonimización, aprovechamiento analítico e inteligencia artificial conforme a los lineamientos distritales.

Largo plazo (12–24 meses)

Entidades del Grupo C:

- Consolidar las capacidades fundacionales de gestión de datos, seguridad digital y privacidad, que les permitan avanzar hacia niveles superiores de madurez conforme a los criterios de evaluación definidos por el Distrito.
- Haber implementado la totalidad de los diez (10) componentes del MVO.

Entidades del Grupo B:

- Consolidar las capacidades de analítica avanzada e inteligencia artificial dentro del Nivel Consolidación definido en el Acuerdo 003 de 2025.
- Exponer al menos un (1) servicio de interoperabilidad documentado y operando bajo los esquemas formales de monitoreo y trazabilidad.
- Implementar mecanismos de anonimización para información sensible.

Entidades del Grupo A:

- Consolidar las capacidades de inteligencia artificial en el Nivel Avanzado, incorporando auditorías algorítmicas periódicas y mecanismos de supervisión continua.
- Exponer servicios de interoperabilidad documentados (APIs) y contribuir al Catálogo Distrital de Servicios de Interoperabilidad.
- Publicar información de transparencia reforzada sobre los sistemas de IA en operación.
- Liderar simulacros distritales de ciberseguridad en coordinación con el CSIRT Distrital.

Pilar transversal: Programa de Fortalecimiento de Capacidades y Cultura Digital (PFCCD)

Como componente que atraviesa todas las fases de la Hoja de Ruta, cada Entidad deberá diseñar e implementar anualmente un Programa de Fortalecimiento de Capacidades y Cultura Digital (PFCCD) en materia de seguridad digital, protección de datos y gestión de datos, con metas diferenciadas por grupo de madurez:

- **Entidades del Grupo C:**
  Capacitación básica en ciberseguridad, manejo de datos personales (Ley 1581 de 2012), uso de formatos estandarizados y sensibilización sobre riesgos digitales.

- **Entidades del Grupo B:**
  Alfabetización en datos maestros, calidad de datos (exactitud, completitud, consistencia, oportunidad, uniformidad), acuerdos de interoperabilidad, gestión de incidentes y gestión de riesgos de seguridad digital.

- **Entidades del Grupo A:**
  Formación en analítica avanzada, inteligencia artificial ética (Niveles Consolidación y Avanzado del Acuerdo 003 de 2025), mentoría interinstitucional y liderazgo en seguridad digital.

El PFCCD deberá incluir:

- Ejercicios periódicos de simulación institucional, realizados al menos dos (2) veces al año, para evaluar la capacidad de respuesta ante incidentes de seguridad digital, crisis de comunicaciones y eventos que afecten la continuidad operativa.

- Un simulacro distrital anual coordinado por el CSIRT Distrital, promoviendo la participación coordinada de Entidades de los Grupos A, B y C.

Además, se sugiere a la Oficina Consejería Distrital de TIC, en coordinación con el DASCD y la Agencia Analítica de Datos, diseñar un plan distrital de formación con contenidos estandarizados y rutas de especialización por rol, como por ejemplo:

Rol	Foco de formación
Administrador de Datos (CDO)	Gobernanza de datos, calidad, datos maestros e interoperabilidad
Oficial de Seguridad (CISO)	MSPI, gestión de riesgos, respuesta a incidentes y auditoría
Analista de datos	Calidad de datos, analítica, IA ética y visualización
Desarrollador	APIs seguras, cifrado, OWASP y DevSecOps
Líder de Planeación	Gobierno de datos, indicadores y gestión de riesgos
Responsable jurídico	Protección de datos personales, acceso a información pública y evaluación de impacto en privacidad

El fortalecimiento de capacidades constituye un habilitador transversal para la implementación de la presente Hoja de Ruta. La consolidación de capacidades técnicas, organizacionales y culturales permitirá que las Entidades evolucionen progresivamente entre los diferentes niveles de madurez, reduciendo la dependencia de iniciativas individuales y promoviendo la institucionalización sostenible de la gestión de datos, la seguridad digital y la protección de la información.

Hoja de Ruta distrital transversal

Complementariamente a las acciones diferenciadas por grupo de madurez, se propone la siguiente Hoja de Ruta distrital transversal, orientada a fortalecer las capacidades, mecanismos de coordinación e instrumentos comunes que deben impulsarse a nivel del ecosistema distrital para apoyar la implementación homogénea de los lineamientos contenidos en este documento.

En este sentido, se sugieren las siguientes acciones para cada horizonte de implementación:

Corto plazo (0 - 6 meses)

Durante esta etapa inicial, se recomienda priorizar la consolidación de las capacidades mínimas de gobernanza, coordinación institucional y control preventivo, con el objetivo de reducir los riesgos más críticos asociados a la gestión y protección de la información distrital.

Las acciones prioritarias sugeridas son:

- **Formalización de las instancias distritales de gobernanza y coordinación:** La implementación de los lineamientos contenidos en este documento requiere la articulación clara entre las siguientes instancias de gobernanza definidas normativamente:
    - El Título 7 del Decreto 640 de 2025 establece los componentes de la Infraestructura de Datos y el modelo de gobernanza correspondiente en el Distrito Capital, definiendo las instancias responsables de la gestión, calidad y aprovechamiento de los datos.
    - El Título 8 del Decreto 640 de 2025 establece el modelo de gobernanza de seguridad digital para el Distrito, definiendo las instancias responsables de la protección de la información y la respuesta ante incidentes.
    - El Acuerdo 001 de 2025 del Comité Distrital de Datos que adopta el reglamento interno del CDD y el Acuerdo 001 de 2025 de la CDTD que crea el Grupo de Ciberseguridad de la CDTD, como instancias especializadas de coordinación.

  Para clarificar la articulación entre estas instancias, se propone el siguiente esquema RACI (Responsable, Aprobador, Consultado, Informado) diferenciado por temáticas clave:

Temática	Responsable (R)	Aprobador (A)	Consultado (C)	Informado (I)
Interoperabilidad	Administrador de Datos de cada Entidad (Anexo 3, Acuerdo 002/2025)	Comité Distrital de Datos (Acuerdo 001/2025)	Oficina Consejería Distrital de TIC	CDTD
Incidentes de seguridad digital	CSIRT Distrital / Oficial de Seguridad de cada Entidad	Grupo de Ciberseguridad CDTD (Acuerdo 001/2025)	UMSD	CDTD / Entidad afectada
Calidad de datos	Administrador de Datos de cada Entidad	Comité Distrital de Datos	Oficina Consejería Distrital de TIC y Ágata	CDTD
Protección de datos personales	Responsable de Privacidad de cada Entidad	Grupo de Ciberseguridad CDTD / Comité Distrital de Datos	Oficina Consejería Distrital de TIC / SIC	CDTD / Titulares de datos
Inteligencia Artificial	Líder de IA / CIO de cada Entidad	Comité Distrital de Datos (Acuerdo 003/2025)	Oficina Consejería Distrital de TIC	CDTD

Este esquema RACI es una propuesta inicial que deberá ser validada y ajustada por la Oficina Consejería Distrital de TIC en coordinación con las instancias de gobernanza definidas y complementada con las acciones que viene realizando el equipo de Ciberseguridad del Distrito.

La formalización de esta matriz contribuirá a que las 63 Entidades del Distrito tengan claridad sobre quién decide, quién ejecuta, quién supervisa y quién reporta en cada dimensión de la transformación digital segura.

- **Identificación y clasificación de los activos críticos de información:** Actualizar el Índice de Información Clasificada y Reservada (IICR) y realizar el inventario inicial de activos de información críticos en las 63 Entidades distritales, priorizando aquellos relacionados con servicios esenciales, atención al ciudadano e infraestructura estratégica.

- **Implementación de controles preventivos mínimos obligatorios:**
  Emitir lineamientos y directrices distritales orientadas a fortalecer la seguridad y privacidad desde las etapas iniciales de los proyectos tecnológicos, incluyendo la obligatoriedad de implementar mecanismos de Autenticación Multifactor (MFA) en accesos críticos y la realización de Evaluaciones de Impacto en Privacidad (PIA) para nuevas iniciativas que involucren tratamiento de datos personales.

- **Definición de los lineamientos institucionales comunes:**
  Establecer criterios y lineamientos distritales mínimos para la gestión de incidentes, clasificación de la información, interoperabilidad segura y protección de datos, con el propósito de promover un lenguaje común y una implementación homogénea entre las Entidades.

- **Inicio del fortalecimiento institucional y cultural:**
  Desarrollar jornadas iniciales de sensibilización y fortalecimiento de capacidades dirigidas a líderes de TI, responsables de datos, oficinas jurídicas y áreas misionales, con énfasis en gobernanza, seguridad digital, privacidad y gestión responsable de la información.

Mediano plazo (6 - 12 meses):

Durante esta etapa, se recomienda consolidar las capacidades operativas definidas en la fase inicial, fortaleciendo los mecanismos de monitoreo, protección de la información, respuesta a incidentes y desarrollo de capacidades institucionales especializadas.

Las acciones prioritarias sugeridas son:

- **Consolidación de la operación distrital de respuesta a incidentes:**
  Poner en funcionamiento las capacidades operativas del CSIRT Distrital, fortaleciendo los procesos de recepción, análisis, priorización, contención y coordinación de incidentes de seguridad digital entre las Entidades del Distrito.

- **Fortalecimiento de los mecanismos de protección de la información:**
  Implementar progresivamente los controles avanzados para la protección de datos sensibles, incluyendo mecanismos de anonimización, seudonimización o enmascaramiento de información en entornos de prueba, analítica y desarrollo, priorizando las Entidades que gestionan mayores volúmenes de información crítica o personal (Ej.: Salud, Movilidad, Hacienda).

- **Evaluación y fortalecimiento de los controles de seguridad:**
  Promover la realización de auditorías internas y ejercicios de evaluación alineados con los estándares reconocidos de seguridad de la información, como ISO/IEC 27001, con el fin de identificar brechas, fortalecer controles y madurar las capacidades institucionales de gestión de riesgos.

- **Desarrollo de capacidades institucionales especializadas:**
  Implementar programas de formación dirigidos a líderes de tecnología, responsables de seguridad, gestores de datos y equipos de apoyo, fortaleciendo competencias relacionadas con ciberseguridad, gestión de incidentes, continuidad operativa, protección de datos y gestión de riesgos.

- **Articulación operativa con los mecanismos distritales de monitoreo:**
  Avanzar progresivamente en la integración de las Entidades con los esquemas distritales de monitoreo y coordinación de incidentes, promoviendo la generación de alertas tempranas, el intercambio de información y la gestión coordinada de eventos de seguridad digital.

Largo plazo (12 - 24 meses):

Durante esta etapa, se recomienda consolidar un ecosistema distrital de datos y seguridad digital caracterizado por altos niveles de interoperabilidad, resiliencia, confianza digital y aprovechamiento responsable de tecnologías emergentes.

Las acciones prioritarias sugeridas son:

- **Evolución hacia arquitecturas de confianza cero (Zero Trust):**
  Avanzar progresivamente hacia modelos de seguridad basados en la verificación continua de identidades, dispositivos, aplicaciones y contextos de acceso, reduciendo la dependencia de los esquemas tradicionales de seguridad perimetral y fortaleciendo la protección de los activos críticos de información.

- **Consolidación de la interoperabilidad segura a nivel distrital:**
  Fortalecer la integración e intercambio seguro de información entre las Entidades del Distrito mediante plataformas, estándares y protocolos interoperables que permitan mejorar la coordinación institucional, reducir la duplicidad de información y optimizar la prestación de servicios al ciudadano.

- **Maduración de las capacidades de monitoreo, resiliencia y respuesta:**
  Consolidar mecanismos avanzados de monitoreo, análisis de amenazas, continuidad operativa y recuperación ante incidentes, fortaleciendo la resiliencia digital del Distrito frente a riesgos tecnológicos emergentes.

- **Implementación de mecanismos de gobernanza para tecnologías emergentes:**
  Incorporar lineamientos, controles y procesos de supervisión para el uso responsable de tecnologías como Inteligencia Artificial, analítica avanzada y automatización, garantizando criterios de transparencia, trazabilidad, explicabilidad, protección de datos y mitigación de sesgos.

- **Fortalecimiento de la confianza digital y la toma de decisiones basada en datos:**
  Promover un ecosistema institucional donde la gestión de datos, la seguridad digital y la innovación tecnológica operen de manera integrada, facilitando la generación de valor público, la toma de decisiones basada en evidencia y el avance progresivo hacia el modelo de “Territorio Inteligente” definido por el Distrito.

La implementación progresiva de las acciones propuestas, bajo un enfoque diferenciado y proporcional al nivel de madurez de cada Entidad, permitirá fortalecer las capacidades institucionales de gestión de datos, privacidad, interoperabilidad y seguridad digital, generando una base común para la toma de decisiones, la gestión de riesgos y la protección de los activos de información.

De manera complementaria, contribuirá a consolidar mecanismos de gobernanza, corresponsabilidad institucional, coordinación interinstitucional y respuesta frente a incidentes, promoviendo una administración pública más resiliente, interoperable y preparada para los desafíos asociados a la transformación digital.

La evolución hacia un “Territorio Inteligente” requiere reconocer que la gestión de datos y la seguridad digital son elementos interdependientes. En consecuencia, el fortalecimiento de las capacidades distritales de monitoreo, prevención, detección y respuesta frente a amenazas deberá considerarse un habilitador estratégico para la protección de los activos de información, la continuidad de los servicios digitales y la generación de confianza en el ecosistema digital del Distrito.

Este enfoque permitirá avanzar de forma ordenada hacia el modelo de “Territorio Inteligente” definido en el Plan Distrital de Desarrollo “Bogotá Camina Segura”, garantizando que el aprovechamiento estratégico de los datos se realice bajo principios de seguridad, privacidad, transparencia y confianza para la ciudadanía.

Asimismo, contribuirá a consolidar una cultura institucional basada en la gestión responsable de los datos, el fortalecimiento de la confianza digital y la generación de valor público mediante el uso ético, seguro e interoperable de la información.