



ANALES DEL CONCEJO DE BOGOTÁ, D.C. PROYECTOS DE ACUERDO

AÑO I N°. 3093 DIRECTORA: ILBA YOHANNA CÁRDENAS PEÑA DICIEMBRE 31 DEL AÑO 2020

TABLA DE CONTENIDO

Pág.

PROYECTO DE ACUERDO No. 439 DE 2020 PRIMER DEBATE “POR MEDIO DEL CUAL SE DICTAN LOS LINEAMIENTOS PARA LA PROMOCIÓN DEL CICLO VIRTUOSO DE LA SEGURIDAD, EL USO Y APROVECHAMIENTO DE LOS DATOS EN BOGOTÁ”	8215
--	------

PROYECTO DE ACUERDO No. 439 DE 2020

PRIMER DEBATE

“POR MEDIO DEL CUAL SE DICTAN LOS LINEAMIENTOS PARA LA PROMOCIÓN DEL CICLO VIRTUOSO DE LA SEGURIDAD, EL USO Y APROVECHAMIENTO DE LOS DATOS EN BOGOTÁ”.

1. OBJETIVO

La presente iniciativa propone definir los lineamientos de una estrategia que deberá implementar la Administración Distrital, para desarrollar procesos que permitan el buen uso y la protección de datos en la construcción de una ciudad inteligente.

2. INTRODUCCIÓN

El contenido del presente proyecto de acuerdo surge como resultado de un proceso de investigación y de la realización de varias mesas de trabajo técnicas en donde estuvieron involucrados, entre otros, los siguientes actores del ecosistema digital:

- Cámara de Industria Digital y Servicios de la ANDI
- Universidad Externado de Colombia
- Grupo de Ciudades inteligentes de Mintic
- Subdirección de Estándares y Arquitectura TI de MINTIC
- Líder de Datos Abiertos de Mintic
- Alta Consejería Distrital TIC
- Centro de Estudios de Política Internacional CEPI.

El diálogo técnico y ciudadano anteriormente mencionado, derivó en un proceso de co-creación del articulado que se presenta en el acápite final de este documento.

3. JUSTIFICACIÓN

El contenido del presente proyecto de acuerdo se sustenta en los elementos conceptuales, técnicos, normativos, y jurisprudenciales que se presentan a continuación:

a. Seguridad digital para ciudades inteligentes.

Las denominadas smart cities o ciudades inteligentes, son las que logran satisfacer en debida forma las necesidades de sus habitantes, para estos fines, se apalancan en el uso de las tecnologías, el aprovechamiento de los datos digitales y a partir de ellas logran un crecimiento armónico con el medio ambiente. En estos modelos de ciudad, se mejora ostensiblemente la prestación de los servicios públicos y se convierte a la urbe en un gran centro de acopio de información interconectada altamente eficiente en sus procesos. Esto se traduce en una mejor calidad de vida para los ciudadanos.

Es por esta razón que, en el marco de la Cuarta Revolución Tecnológica, los ciudadanos y las organizaciones apelan al uso de la tecnología y la incorporan en nuevas formas de relacionarse con el entorno para incrementar su productividad, para ser más competitivos en los negocios, para satisfacer necesidades propias y para generar valor. La literatura propone a la tecnología como un elemento protagonista para el despliegue de las ciudades inteligentes. Se ha señalado que la infraestructura más básica de tecnologías de la información, requerida está relacionada con canales de fibra óptica, redes inalámbricas, puntos de acceso y otros sistemas de información, que son los elementos tradicionales del sistema de TI (Vitunskait et. al, 2019).

Sin embargo, de acuerdo con el texto denominado “*Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership*”, de manera explícita para una ciudad inteligente, la infraestructura incluye sensores, dispositivos de acceso al consumidor final, además de un sinfín de posibilidades tecnológicas que permiten que los usuarios se conecten con todas las funcionalidades de la ciudad.

Dicha infraestructura implica que se empiece a diseñar un modelo de ciudad que se convierta en un centro de operaciones capaz de recepcionar los datos digitales que se producen a diario y que son aportados por los ciudadanos a través de sus dispositivos móviles, laptops y relojes inteligentes, entre otros, con el fin de aprovecharlos para el funcionamiento de la ciudad. Para estos propósitos se requiere adecuar un gran centro de almacenamiento de datos, con capacidad de procesamiento en tiempo real y destinados a dar las soluciones que requiere la ciudad.

Entendiendo esta realidad, el Plan de Desarrollo del Distrito Capital 2020-2024”, incorporó el Programa Estratégico: 16 Ciudad Inteligente. Así como también el programa 54 Transformación digital y gestión de TIC para un territorio inteligente, que se refiere a la generación de las capacidades necesarias para realizar la adecuada coordinación y articulación de los proyectos de transformación digital y gestión de TIC en el Distrito. Estas capacidades están centradas en talento humano especializado, esquemas de

acompañamiento, campañas de comunicación y difusión, habilitación de tecnologías, laboratorios de innovación y demás elementos que permitan generar valor a las iniciativas TIC de los sectores¹.

Quizá, la razón por la cual, urge que la Administración Distrital acelere estos procesos, va encaminada a mejorar la percepción de Bogotá como ciudad inteligente en el mundo. Esto encuentra sustento en el análisis del estudio de ciudades inteligentes del *IESE Cities in Motion Strategies*, del cual se se desprenden los siguientes datos, obsérvese como Bogotá ocupa el puesto 117, Medellín, el puesto 134, Cali el puesto 148; mientras que Hong Kong, está en el puesto 11, Singapur está en el puesto 7, París en el puesto 4 y Londres, está en el primer lugar, entre más de 137 ciudades, con lo cual se establece fácilmente que se requiere recorrer un largo camino para ubicar a la capital del país como un referente de innovación y que debe existir voluntad política para lograrlo.

Según la Unión Internacional de Telecomunicaciones, ITU, por sus siglas en inglés, las ciudades inteligentes sostenibles necesitan infraestructura de telecomunicaciones que sea estable, segura, fiable e interoperable para dar soporte al ingente volumen de aplicaciones y servicios basados en las TIC².

De acuerdo con esta misma organización, los recientes adelantos en la tecnología de Internet de las cosas (IoT), la inteligencia artificial (IA) y las redes y contadores eléctricos inteligentes están impulsando y apoyando el desarrollo de ciudades inteligentes sostenibles en todo el mundo.

A continuación se presentan estos avances desarrollos que caracterizan a una ciudad inteligente y que en todos los casos se sustenta en el uso y aprovechamiento de datos:

La IoT —que consiste en la red en rápida expansión de dispositivos con sensores y programas informáticos integrados que se conectan entre sí y comparten datos— permite que miles de millones de dispositivos y objetos equipados con sensores inteligentes se conecten entre sí, recopilen información en tiempo real y envíen estos datos, a través de una comunicación inalámbrica, a sistemas de control centralizados. Estos, a su vez, gestionan el tráfico, reducen el consumo de energía y mejoran muy diversas operaciones y servicios urbanos.

La IA permite analizar enormes conjuntos de datos para revelar patrones, que luego se emplean para informar y mejorar la toma de decisiones municipales.

Las redes eléctricas inteligentes - es decir, las redes de suministro eléctrico que utilizan tecnología de comunicación digital para detectar y reaccionar a las variaciones de consumo locales - ayudan a optimizar el consumo de energía en las ciudades. Los contadores y sensores inteligentes, equipados

¹ Acuerdo 761 de 2020 Por medio del cual se adopta el Plan de desarrollo económico, social, ambiental y de obras públicas del Distrito Capital 2020-2024 “Un nuevo contrato social y ambiental para la Bogotá del siglo XXI”: Recuperado de: <https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=93649>

² Recuperado de: <https://www.itu.int/es/mediacentre/backgrounders/Pages/smart-sustainable-cities.aspx>

con direcciones de protocolo de Internet, pueden comunicar al proveedor de energía información sobre el consumo del usuario final, dando a este último un mayor control sobre su consumo.

Mientras que las redes 3G y 4G utilizadas hoy en día por los teléfonos móviles plantean una serie de problemas a la hora de dar soporte a los diversos servicios necesarios para las aplicaciones de ciudades inteligentes y sostenibles, el desarrollo de la tecnología 5G, es decir, la quinta generación de tecnologías móviles, tiene el potencial de conectar de forma fiable los dispositivos a Internet y a otros dispositivos, transportar los datos rápidamente y procesar un gran volumen de datos reduciendo los tiempos.

Ahora bien, es cierto que la tecnología es un componente clave, primero deben existir una serie de habilitadores que permitan su correcta y segura apropiación para impulsar ciudades inteligentes. Privilegiar la elección de la capa tecnológica de la ciudad antes de reflexionar en torno a asuntos trascendentales como la seguridad digital sería un craso error que pondría en situación de riesgo a un ecosistema tan complejo como el que compone cualquier territorio.

Frente a esto, como lo señala el Ministerio de Tecnologías de la Información y las Comunicaciones (2017), indicó que además del en otros escenarios se ha incrementado el uso de la tecnología con fines delictivos o para generar amenazas informáticas; este propósito busca afectar otras infraestructuras tecnológicas, sistemas de información financieros, personas e, incluso, llegar a impactar la economía de toda una nación.

b. Incidentes de seguridad digital

El estudio Tendencias del Cibercrimen 2019-2020, presentado por el Tanque de Análisis y Creatividad de las TIC - TicTac de la CCIT y su programa SAFE en asocio con la Policía Nacional - Centro Cibernético Policial, junto a aliados estratégicos como Absolute, Cisco, Claro, Fortinet McAfee y Microsoft, presentan las cifras y modalidades de los ciberdelitos en 2019 y las tendencias que enfrentan las empresas colombianas y los ciudadanos en 2020, panorama que no es lejano al análisis que agencias de carácter internacional como el EC3 (Centro Europeo Contra la Cibercriminalidad de EUROPOL) han identificado a nivel mundial. (Yohai, 2019)

El estudio presenta los datos estadísticos de las diferentes modalidades de ciber delitos a los que está expuesto el público, y que han sido denunciados a través de 15.948 denuncias y reportes realizados por empresas y ciudades al Centro Cibernético Policial (CECIP)

Mediante la elaboración de un instrumento interno aplicado a estos reportes delictivos fueron identificados los principales vectores de infección utilizados por los ciber delincuentes, así como las técnicas de ofuscación del malware con el cual afectan a las empresas y ciudadanos en el país.

El estudio “Tendencias Cibercrimen Colombia 2019-2020” se centra en determinar cuáles son los delitos informáticos que más afectan a los colombianos, por lo que da las siguientes cifras de los cinco principales delitos informáticos más comunes y reportados en el país de la siguiente manera:

1. El delito informático más denunciado en Colombia es el hurto por medios informáticos con un total de 31.058 casos, los cibercriminales saben que el dinero está en las cuentas bancarias y por eso buscan comprometer los dispositivos utilizados en la interacción entre usuarios y banca.
2. En segundo lugar, se encuentra la violación de datos personales con 8.037 casos. Este dato revela que la segunda amenaza en Colombia para empresas y ciudadanos es el Robo de Identidad.
3. El tercer delito más denunciado es el acceso abusivo a sistema informático con 7.994 casos, y esto se explica en razón a que, en las fases primarias de los ciberataques, los cibercriminales buscan comprometer los sistemas informáticos logrando ganar el acceso a los mismos.
4. En cuarto lugar, con 3.425 casos se encuentra la transferencia no consentida de activos, conducta criminal que facilita al atacante sustraer el dinero o transferir valiosos activos financieros de las víctimas.
5. Finalmente, en quinto lugar, se sitúa el delito de uso de software malicioso con 2.387 casos.

Ahora en lo concerniente a las ciudades más afectadas por ciber delincuentes en 2019, el estudio “Tendencias Cibercrimen Colombia 2019-2020” ubica a los principales centros urbanísticos del país con el 55 % de casos de ciberdelitos, entre los que se encuentra Bogotá con 5.308 casos, Cali con 1.190 casos, Medellín con 1.186 casos, Barranquilla con 643 casos y Bucaramanga con 397 casos. Estas ciudades son el foco de ataques por parte de ciber delincuentes por su desarrollo económico que motiva e influye en los objetivos de los ciber criminales que enfocan su actuar hacia PYMES, entidades financieras y grandes compañías con asiento en estas ciudades.

El documento CONPES 3995, que trata la Política Nacional de Confianza y Seguridad Digital, también plantea cifras preocupantes frente a ciberataques en Colombia entre los años 2017 y 2019 y compara dichas cifras con las de ciberataques realizados a las principales potencias mundiales, esto según el reporte Estado de Internet 2019, que afirma que entre noviembre de 2017 y septiembre de 2019, en Colombia se originaron alrededor de 536 millones de ataques (contados entre inicio de sesión malicioso y ataques a aplicaciones web). Por su lado, en Estados Unidos se originaron alrededor de 26.800 millones, en Rusia 7.200 millones, en China 3.200 millones, en India 3.120 millones, en Alemania 2.330 millones y en Japón 920 millones de este mismo tipo de ataques. Si consideramos que el entorno digital es un entorno que nos conecta con el resto del mundo, entonces hay un gran número de ataques a los cuales se encuentran expuestos los ciudadanos en Colombia, no sólo por los ataques que se originen en el país, sino por la sumatoria de ataques que se originan globalmente. Indudablemente esto lleva a una sensación de desconfianza en el entorno digital. (Akamai, 2019)

El Documento CONPES 3995, también centra su estudio en las debilidades en las capacidades en seguridad digital de los ciudadanos del sector público y del sector privado, frente al sector público el

documento se refiere al Global Cyber Security Index (Unión Internacional de Telecomunicaciones (UIT), 2018), mide el compromiso de los 175 países evaluados en torno a la ciberseguridad y generando un ranking mundial al respecto. Esta evaluación se realiza a través de 5 pilares (legal, técnico, organizacional, construcción de nuevas capacidades y cooperación), que describen adecuadamente las capacidades que se deben generar en el país para mejorar la confianza y la seguridad digital. En este índice, Colombia pasó del puesto 46 en la versión 2017 al puesto 73 en la versión 2018, perdiendo así varias posiciones en corto tiempo, lo cual evidencia que Colombia no ha mejorado sus capacidades para dar respuesta oportuna a incidentes y amenazas en seguridad digital. (CONPES 3995, 2019)

Por otro lado, el NCSI22 es un índice que mide la preparación de los países para prevenir amenazas y gestionar incidentes, relacionados con seguridad digital. La medición de este índice se enfoca en 4 aspectos relacionados con la implementación en ciberseguridad: (i) legislación vigente, (ii) unidades establecidas, (iii) marco de cooperación y (iv) resultados. (National Cyber Security Index - NCSI, 2020). En los resultados de dicho índice Colombia obtiene un puntaje global de 46,75 sobre un total de 100, lo que muestra una baja preparación en seguridad digital.

Esto respecto al sector Público en Colombia, ahora, en lo concerniente al sector privado el (DNP, 2019) se refiere al Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales, analizó las medidas de seguridad implementadas para recolectar, almacenar, usar, circular o tratar datos personales en 31.41025 empresas (entre privadas, sin ánimo de lucro y mixtas) del país (Superintendencia de Industria y Comercio - SIC, 2019). Este estudio refleja que el 44 % de las empresas que hacen parte del estudio, tienen un nivel de implementación menor o igual al 25 % de las medidas apropiadas y efectivas para garantizar la seguridad de los datos personales y sólo el 15 % tienen un nivel de implementación igual o superior al 76 %, de todos los requerimientos de seguridad emitidos por la SIC. Esto muestra una falta de preparación para garantizar la seguridad de los datos personales y por ende una ausencia de capacidades al respecto.

Ahora bien, en el mundo viene desarrollándose una tecnología altamente competitiva en la protección de datos digitales y que permitiría superar en gran medida todos los problemas descritos en incisos precedentes, se trata de la *blockchain*. Su funcionamiento consiste en la administración de una gran base de datos a cargo de varios usuarios que la auditan entre sí en tiempo real y que está contenida en bloques de transacciones descentralizadas y enlazadas, permitiendo el registro inamovible de todo movimiento que se realice en ella (Preukschat, 2017).

Uno de los elementos más innovadores en la materia son sus complejos algoritmos y la eliminación de reprocesos, haciendo muy eficiente el sistema y reduciendo los costos (Ocariz, 2017). Ya existen en el mundo varios casos de éxito como la isla de Malta en Europa, donde gran parte de sus procesos gubernamentales y la prestación de servicios públicos se realiza a través de esta tecnología.

En conclusión, se evidencia que en Colombia hay deficiencias en todo el conjunto de las capacidades relacionadas con la seguridad digital, por parte de los ciudadanos, del sector público y del sector privado. Esto causa que el país presente bajos niveles de preparación y de avance en la materia, lo

que a su vez incrementa la vulnerabilidad del país ante ataques y amenazas cibernéticas, deteriorando la confianza y el normal desarrollo de nuestro entorno digital (DNP, 2019).

c. **Evaluaciones de impacto de protección de datos**

De acuerdo con la Agencia Española de Protección de Datos, es fundamental realizar evaluaciones de impacto a la protección de datos. Por lo que se requiere desarrollar metodologías que permitan evaluar de manera anticipada los potenciales riesgos a los que están expuestos los datos de acuerdo a las actividades que se llevan a cabo con ellos.

Algunas sugerencias son:

1. Definir el ciclo de vida de los datos.
2. Identificar amenazas y riesgos (Desastres naturales, errores y fallos de programación, ataques intencionados, acceso ilegítimo a los datos de confidencialidad, entre otros).
3. Definir un plan de acción para enfrentar estos riesgos.

De otro lado, en este proceso es vital importancia que la administración presente informe de las medidas adelantadas para mitigar los riesgos, además de examinar periódicamente el tratamiento del plan de acción. Así como también documentar y sobre todo hacer públicas las decisiones que se tomen frente al uso de los datos.

d. **Disposiciones del CONPES de explotación de datos.**

La década de los cincuenta fue caracterizada por dar inicio a la llamada primera revolución digital, también llamada tercera revolución industrial por la introducción de la electrónica en las principales economías del planeta. Esta revolución resalta por el desarrollo de los sistemas digitales, las telecomunicaciones y el aumento exponencial de poder de procesamiento, situación que permitió nuevas formas de generar, procesar y compartir información (World Economic Forum, 2016)

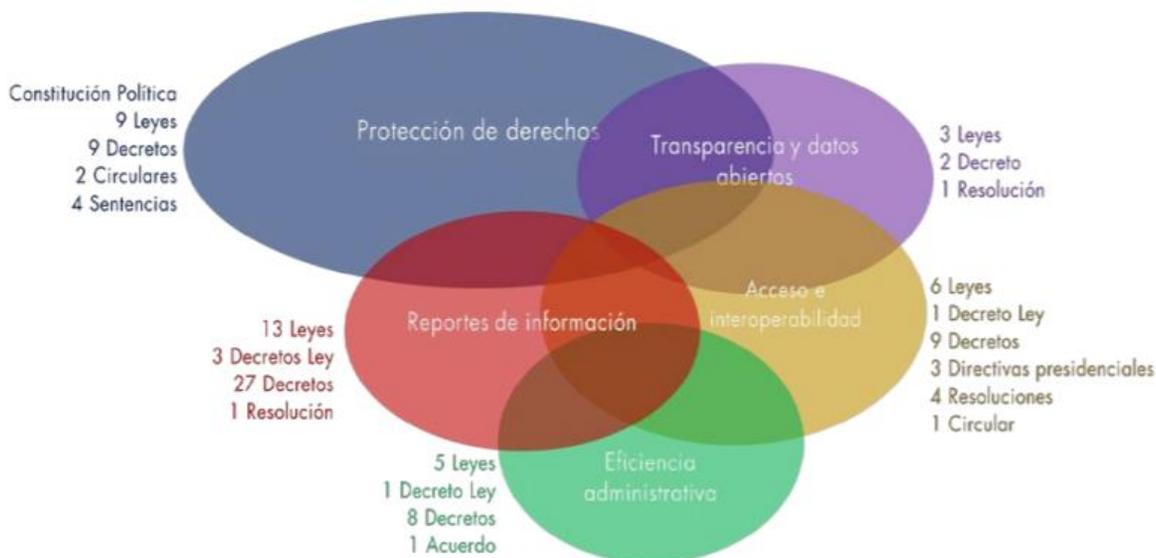
Durante la década de los ochentas se da un avance monumental en materia de datos por medio de la creación de la primera base de datos digital para almacenar los datos de manera manual, llegando así a un proceso más ágil en materia de procesamiento y generación de información.

Acabando el siglo XX y durante los primeros años del siglo XXI se llega a una nueva era de la digitalización, la popularidad del Internet en todas las esferas mundiales culmina en una nueva forma de administrar datos de manera masiva. Este tipo de administración de datos se hizo según el World Economic Forum de manera consciente e inconsciente. La primera de estas modalidades por medio del uso de sistemas de información y bases de datos entre otros; el segundo por medio de rastros digitales derivados del uso de redes sociales, la navegación en Internet, el uso del teléfono celular y similares. Todo esto en conjunto con los nuevos avances tecnológicos en materia de digitalización permitieron identificar los datos como un activo de vital importancia para la nueva revolución industrial que se gestaba a pasos exponenciales.

Desde hace aproximadamente 20 años en Colombia, se reconoció la necesidad de usar las tecnologías de la información y las comunicaciones con el fin de aumentar la eficiencia en el desarrollo de los procesos y la gestión gubernamental. Sin embargo, no fue sino hasta la expedición del Plan Nacional de Desarrollo 2014-2018 que se reconoció puntualmente la importancia de los datos como un activo para generar valor social y económico.

De acuerdo con el documento CONPES 3920, sobre la Política Nacional de Explotación de Datos (Big Data), el país ha avanzado en la provisión de condiciones normativas e institucionales para que las entidades públicas intercambien información y publiquen los datos de su gestión. Adicionalmente, existe un régimen robusto de protección de datos personales con controles fuertes para su garantía. Sin embargo, a pesar de los avances normativos en materia de datos, el país todavía se queda limitado en el aprovechamiento de los niveles de datos digitales que manejan sus entidades públicas, situación que presenta un obstáculo en el aprovechamiento de datos alrededor del territorio, puesto que no se está haciendo uso de estos de manera adecuada, y no se están tomando en cuenta los beneficios que pueden generar en materia económica y de generación de valor social.

En Colombia la realización de los procesos de generación, recolección, agregación, compartición, explotación e innovación para aprovechar datos se encuentran mediados por diversas disposiciones jurídicas que conforman el marco relevante vigente para la explotación de datos. Estas se agrupan en cinco grandes categorías de acuerdo con las materias reguladas y que el documento CONPES 3920 agrupa en la siguiente tabla:



Fuente: DNP (2018).

Las disposiciones jurídicas con impacto en la explotación de datos señaladas en la tabla se agrupan en cinco regímenes, según el tema regulado por cada una, así: (i) protección de derechos, esto es, límites y garantías que deben desplegarse para el tratamiento de datos personales y privados; (ii)

transparencia y datos abiertos, que corresponde a la publicidad de las actuaciones de las entidades públicas, el derecho de acceso a la información pública y la necesidad de divulgación activa; (iii) acceso e interoperabilidad, que define condiciones mínimas para que las entidades públicas y privadas que desarrollan funciones públicas establezcan mecanismos para permitir el uso de datos entre sí; (iv) eficiencia administrativa, es decir, la gestión de los documentos generados por las entidades públicas y las privadas que prestan funciones públicas, así como aumento de la generación de documentos digitales para eliminar los soportes en papel y disminuir los trámites solicitados al ciudadano; y (v) reportes de información, que corresponde a los reportes de datos que las entidades privadas, la academia y los ciudadanos deben suministrar periódicamente a las entidades públicas en el marco de sus competencias, a los particulares que desarrollan funciones públicas, así como aquellos que las entidades públicas deben realizar (Documento CONPES 3920, 2018)

Este entramado jurídico demuestra un claro avance en la materia por parte del país, sin embargo, este marco tan robusto carece de armonización para habilitar los procesos de explotación de datos para la generación de valor económico y social, considerando que se compone de disposiciones y precedentes jurídicos que fueron expedidos de manera independiente con el fin de regular situaciones sociales concretas, en momentos y sectores específicos.

Como lo demuestra el Documento CONPES 3920, actualmente hay varios países que están aprovechando los grandes beneficios de apostar por una política de explotación de datos, por su potencial en impulsar el crecimiento económico, la productividad pública y privada e incidir en la preparación para la economía digital, donde es fundamental que las empresas hagan parte de las redes digitales, porque la mayoría de los bienes de mercado pueden ser digitalizados, permitiendo que se proliferen con facilidad, a un costo de escalabilidad cercano a cero, porque cada nodo adicional de una red digital incrementa el valor para los demás, de modo que la red genera su propio crecimiento (World Economic Forum, 2016).

Referente	Año y documento para adopción de la estrategia	Objetivos de la política pública
Estados Unidos	2012: Iniciativa de investigación y desarrollo en <i>Big Data</i>	• Promover habilidades para el aprovechamiento de datos en las agencias gubernamentales.
	2016: Plan Federal Estratégico de Investigación y Desarrollo en <i>Big Data</i>	• Explotar datos para acelerar descubrimientos científicos e innovación y promover el crecimiento económico.
Unión Europea	2013: Consejo Europeo 24/25 Conclusiones	• Promover la economía digital, la innovación y los servicios como motores del crecimiento y el empleo.
	2014: Comunicación de la Comisión al Parlamento	• Crear un mercado de datos único.

EI

	Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Hacia una economía de los datos próspera	
Australia	2012: Estrategia australiana de TIC del Servicio Público 2012-2015 2013: La estrategia de <i>Big Data</i> para el servicio público de Australia: mejorar la comprensión mediante un aumento en el análisis de datos	<ul style="list-style-type: none"> • Aumentar la productividad nacional y del sector público, mediante la toma de mejores decisiones de política pública, que se basen en datos y en mejor información. • Los datos son reconocidos como un activo nacional para el Gobierno y los ciudadanos.
Corea del Sur	2013: Informatización nacional para alcanzar la sociedad del conocimiento y la información 2013: Gov 3.0 2013: Plan maestro de <i>Big Data</i>	<ul style="list-style-type: none"> • Liderar la economía creativa a través de la informatización, con un Gobierno proactivo, científico y capaz en el que convergen datos públicos y privados.
Reino Unido	2013: Aprovechando la oportunidad de los datos. Una estrategia para la capacidad del Reino Unido 2017: Estrategia de transformación del Gobierno: mejor uso de los datos	<ul style="list-style-type: none"> • Extraer conocimiento y valor de los datos para el beneficio de los ciudadanos, el sector privado, la academia y el sector público. • Desarrollar la capacidad de datos, es decir, la habilidad de consumidores, negocios y academia de acceder y compartir datos apropiadamente. Se compone de capital humano, infraestructura y datos. • Define las prioridades de Gobierno hasta 2020, centrado en la remoción de barreras para el uso de datos públicos, aumentar las capacidades en ciencia de datos al interior del Gobierno, definir herramientas para la seguridad en el uso de datos y aumentar la apertura.
Francia	2014: Industria del futuro	<ul style="list-style-type: none"> • Propone nueve soluciones industriales del país para modernizar la base de producción: nuevos recursos, ciudades inteligentes, eco-movilidad, transporte, medicina, economía de datos, dispositivos inteligentes, confianza digital, y elección inteligente de alimentos. • Mejor manejo y apropiación de los datos por las compañías y el sector público. • Crear un ecosistema de economía de datos.
Japón	2013: Declaración para ser la nación más avanzada en tecnologías de información (TI)	<ul style="list-style-type: none"> • Crear una sociedad que promueve la innovación y generación de nuevos servicios, industrias y crecimiento, mediante el uso de datos abiertos y <i>Big Data</i>.

Documento CONPES 3920, presenta una tabla donde muestra los avances legislativos

China	2015: Plataforma para la acción en la promoción del desarrollo de <i>Big Data</i>	<ul style="list-style-type: none"> • Unificar los datos gubernamentales para facilitar servicio al ciudadano. • Aumentar los datos abiertos para promover innovación industrial, nuevos negocios y reestructuración económica.
-------	---	--

e. Diagnóstico de Colombia y Bogotá frente apertura, uso y aprovechamiento de datos.

Los datos son uno de los recursos más valiosos en las sociedades, economías y gobiernos actuales. Las políticas de datos gubernamentales abiertos (OGD) se basan en ideas y principios que se centran en hacer que los datos de los organismos públicos estén disponibles para todos en formatos abiertos, gratuitos y accesibles. Las prácticas de los países de la OCDE muestran que el acceso a los datos gubernamentales puede fomentar la participación social, las oportunidades comerciales y la innovación, creando valor agregado a partir de la información existente.

Hoy los gobiernos en todo el mundo tienen la oportunidad de aprovechar los beneficios de los datos que han sido recolectados o producidos por las instituciones públicas y privadas o no gubernamentales (Ubaldi, 2013).

Lo anterior, con el propósito de generar valor a partir del uso de esos datos. De ahí lo importante de formular políticas que promuevan la apertura, la interoperabilidad, el procesamiento, el intercambio y la reutilización de los datos en el Distrito, para que puedan ser aprovechados por parte de las instituciones públicas, pero también por parte de terceros.

De acuerdo con las recomendaciones del Comité de Gobernanza Pública de la OECD (OECD, 2014), es recomendable que el gobierno genere una cultura impulsada por datos en el sector público a través de dos aspectos:

1. Desarrollar marcos para habilitar, orientar y promover el acceso, uso y reutilización de la creciente cantidad de evidencia, estadísticas y datos relacionados con operaciones, procesos y resultado para:
 - a. Aumentar la apertura y la transparencia
 - b. incentivar el compromiso ciudadano en la formulación de políticas, la creación de valor público, el diseño y la entrega de servicios

2. Equilibrar la necesidad de proveer datos oficiales oportunos para entregar información confiable, gestionar los riesgos del mal uso de datos relacionados con su creciente disponibilidad en formatos abiertos, lo que quiere decir que debe permitirse su uso y reutilización, así como la posibilidad de que actores no gubernamentales reutilicen y complementen los datos con el fin de maximizar el valor público económico y social

f. Consideraciones éticas para orientar el uso de la proximidad digital tecnologías de seguimiento para el seguimiento de contactos COVID-19 OMS

- Debe haber un equilibrio entre los beneficios y los riesgos asociados con la recopilación, el proceso y el intercambio de datos personales.
- Las aplicaciones digitales deben caracterizarse por tener privacidad por diseño, es decir, la seguridad es proactiva y no reactivo; preventiva y no correctiva.

- Solo conservarse durante el tiempo que sea necesario para cumplir con el propósito específico para el que fueron recopilados.
- El ciudadano debe tener consentimiento totalmente informado y explícito sobre el uso de sus datos.
- Encriptar datos, es decir, cifrar los datos y anonimizar la información personal.
- Garantizar a los ciudadanos sus derechos fundamentales, incluido el derecho de acceso a sus datos personales, el derecho de borrado y el derecho a ser informados sobre los fines del procesamiento y con quién se comparten esos datos.

g. Creación de la nueva Agencia Analítica de Datos del Distrito aprobada en el Plan de Desarrollo Distrital (2020- 2024) “Un Nuevo Contrato Social y Ambiental para la Bogotá del Siglo XXI”.

El nuevo Plan de Desarrollo Distrital 2020- 2024 “*Un Nuevo Contrato Social y Ambiental Para la Bogotá del Siglo XXI*” presenta un artículo con una propuesta innovadora que cambiará la forma en la que se analizan, interpretan y utilizan los datos de la ciudad y de sus habitantes, esto con el fin de que la ciudadanía confíe más en la transparencia en las acciones de la Administración y al mismo tiempo, hacer de Bogotá una ciudad más inteligente (Medina, 2020)

Esta visión innovadora se logrará gracias a la materialización de los objetivos de la Administración, la aprobación del Consejo Distrital y el liderazgo de la Alta Consejería de TIC y la Empresa de Telecomunicaciones de Bogotá ETB en materia de manejo de datos. La nueva Agencia de Analítica de Datos del Distrito está contemplada en el artículo 145 del nuevo Plan de Desarrollo Distrital y emerge como una necesidad para una ciudad que necesita entrar a la nueva realidad mayor digitalización, más conexión y por supuesto más virtualidad.

De acuerdo al articulado la agencia será una sociedad por acciones vinculada a la Secretaría General de la Alcaldía Mayor y encargada de “los procesos inherentes a la analítica de datos como la validación, recolección, integración, almacenamiento, depuración, estandarización, tratamiento, procesamiento, enriquecimiento, visualización y analítica multifinanciaría de datos estructurados y no estructurados del Distrito Capital e información pública y privada, preservando la observancia de los principios y normas de protección de datos personales, de conformidad con lo dispuesto en las Leyes 1581 de 2012 y 1712 de 2014, y demás normas que regulan la materia”.

Ágata es el nombre que tomó la primera Agencia de Analítica de Datos del país, una apuesta con varios proyectos a futuro de acuerdo con el portal Bogotá así vamos, entre los que se encuentran:

- Gestión de servicios sociales con una visión de 360 grados de los ciudadanos, así como respuestas automáticas a solicitudes en redes sociales.
- Disminución del consumo de energía del alumbrado público con el uso de sensores inteligentes
- Lograr que los comerciantes informales tengan acceso a microcréditos del sistema financiero para evitar que sean sujetos de usura.

- Conectar datos de las cámaras de seguridad de la ciudad con la información sobre delitos para que a partir de la analítica se pueda avisar a las autoridades y que estas puedan actuar de manera predictiva para atacar el crimen.
- Uso de nuevas tecnologías para luchar contra la corrupción.
- Promoción de tecnologías como el blockchain para asegurar datos e información de contratación y gasto público.

Gracias a esta nueva apuesta por la innovación, Bogotá se convertirá en la primera ciudad del país en centralizar y administrar los datos de los sectores educación, cultura, movilidad, salud, medio ambiente, planificación urbana y atención al ciudadano con el fin de garantizar el uso eficiente de estos datos y fortalecer los sistemas que integran la información de estos sectores, todo esto en beneficio de los Bogotanos (Sáenz, 2020).

h. Formación y educación continua en protección y aprovechamiento de datos para ciudadanos y funcionarios públicos del Distrito.

El aumento de la digitalización y el uso de medios virtuales por las personas en Bogotá y el mundo, presentan un nuevo desafío para los que buscan seguir el ritmo de la más reciente revolución industrial, enfocada principalmente en las nuevas tecnologías y el uso y el aprovechamiento de estas en los diferentes sectores del Distrito.

La globalización, el proceso que ha generado una transformación económica, cultural, social y política, haciendo que todos los países, así como las personas que los integran, estén interconectados unos con otros gracias a los avances en tecnologías de la información. Un ejemplo de esto es la llegada del internet al panorama mundial, situación que ha permitido tener una visión más amplia de lo que depara el futuro en aprovechamiento y manejo de las nuevas tecnologías que avanzan cada vez más rápido.

Ahora, uno de los dilemas que surge con la globalización y la nueva era de la tecnología, es el manejo y uso de los datos que genera el uso de estas. Herramientas como el internet y las redes sociales han presentado un aumento exponencial en los usuarios que las utilizan. Según Datereportal para el 2020, más de 4,5 mil millones de personas en el mundo usan Internet, 3,8 mil millones son usuarias de redes sociales y 5,19 mil millones de personas usan teléfonos móviles. Con respecto al año 2012, la cifra de penetración a Internet a nivel mundial pasó del 30 % al 60 %, y la de redes sociales pasó del 22 % al 49 %.

Considerando la gran cantidad de usuarios de este tipo de herramientas tecnológicas en el mundo, que solo seguirán aumentando, urge que las autoridades velen por el buen uso y aprovechamiento de los datos que se aportan constantemente en estas y sancionen cualquier comportamiento que pretenda usar los datos de manera fraudulenta.

Aquí es donde nace la necesidad de que, tanto ciudadanos, como autoridades y servidores públicos se capaciten en el uso, aprovechamiento y por supuesto protección de datos, esto con el fin de

adelantarse a la delincuencia, que también sigue evolucionando y desarrollando nuevas e ingeniosas tretas para engañar y aprovechar la información de los usuarios para fines ilícitos.

Así como los temas de seguridad en el manejo de datos presentan una gran preocupación, también sirven como impulso para lograr esa evolución tecnológica que tanto requiere el país en este momento, y los datos, su uso, aprovechamiento y explotación pasarán a ser un tema central en esta evolución, considerando que se han convertido en activos estratégicos para la generación de valor social y económico tanto en el sector público como en el privado. Los aportes del Big Data a la creación de valor para el sector público son diversos, y se orientan a mejorar la prestación de servicios al ciudadano, acompañar el proceso del ciclo de política pública y mejorar los niveles de eficiencia (McKinsey Global Institute, 2016)

El aprovechamiento de grandes cantidades de datos en el sector público trae oportunidades para generar evidencia en el diseño, implementación y seguimiento de los programas, proyectos y políticas, pero también importantes desafíos. Un ejemplo de esto como lo menciona el DNP en el CONPES 3920, es la necesidad de contar en el país con las competencias necesarias para el análisis y explotación de datos, así como la incorporación de la analítica de datos en la agenda operativa y misional del Gobierno y de las entidades públicas, avances que progresivamente han avanzado, pero que todavía requieren de mucho trabajo.

Es por lo anterior que se requiere de personas capacitadas en la protección de datos personales, así como en el uso aprovechamiento y explotación de los datos para la gestión pública, esto con el objetivo de afrontar estos nuevos desafíos que presentan las nuevas tecnologías, esta evolución que no va a dar marcha atrás y para la que la administración debe estar preparada de cara a la cuarta revolución industrial.

4. ANTECEDENTES NORMATIVOS.

CONSTITUCIÓN POLÍTICA

ARTÍCULO 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley (...)

ARTÍCULO 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación.

Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.

ARTÍCULO 74. Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley.

El secreto profesional es inviolable.

LEYES

- Ley 527 de 1999 – Validez jurídica y probatoria de la información electrónica;
- Ley 594 de 2000 – Ley General de Archivos – Criterios de Seguridad
- Ley 679 de 2001 – Pornografía Infantil – Responsabilidad ISPs
- Ley 962 de 2005 – Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas
- Ley 1150 de 2007 – Seguridad de la información electrónica en contratación en línea
- Ley 1266 de 2008 – Habeas data financiera, y seguridad en datos personales
- Ley 1273 de 2008 – Delitos Informáticos y protección del bien jurídico tutelado que es la información
- Ley 1341 de 2009 – Tecnologías de la Información y aplicación de seguridad
- Ley 1437 de 2011 – Procedimiento Administrativo y aplicación de criterios de seguridad
- Ley 1480 de 2011 – Protección al consumidor por medios electrónicos. Seguridad en transacciones electrónicas
- Ley 1581 de 2012 – Ley estatutaria de Protección de datos personales
- Ley 1623 de 2013 – Ley de Inteligencia – Criterios de seguridad
- Ley 1712 de 2014 – Transparencia en el acceso a la información pública
- Ley 1928 de 2018 – Por medio de la cual se aprueba el convenio sobre la ciberdelincuencia, adoptado el 23 de noviembre de 2001 en Budapest

DECRETOS

- Decreto 1151 de 2008- Estrategia de Gobierno en Línea

Decreto 2364 de 2012 – Firma electrónica

- Decreto 2609 de 2012 – Expediente electrónico
- Decreto 2693 de 2012 – Gobierno electrónico
- Decreto 1377 de 2013 – Protección de datos personales
- Decreto 1510 de 2013 – Contratación Pública electrónica
- Decreto 333 de 2014 – Entidades de certificación digital
- Decreto 2573 de 2014- Gobierno en Línea

Decreto 1008 de 2018- Política de Gobierno Digital

JURISPRUDENCIA

Sentencia de tutela T-729/02, primera en referirse a la materia de protección de datos y los principios para su tratamiento, que posteriormente se incorporaron a las Leyes Estatutarias 1266 de 2008, 1581 de 2012, 1621 de 2013, 1712 de 2014 y 1755 de 2015.

5. COMPETENCIA DEL CONCEJO.

La Constitución Política de Colombia en su Artículo 313, numeral 1, establece que corresponde a los concejos reglamentar las funciones y la eficiente prestación de los servicios a cargo del municipio. Así mismo, el Decreto Ley 1421 de 1993 en su Artículo 12, numeral 1, estipula que corresponde al Concejo Distrital, de conformidad con la Constitución y la Ley, dictar las normas necesarias para garantizar el adecuado cumplimiento de las funciones y la eficiente prestación de los servicios a su cargo.

6. BIBLIOGRAFÍA

- Acuerdo No. 761 de 2020, [Concejo de Bogotá, D.C.]. *POR MEDIO DEL CUAL SE ADOPTA EL PLAN DE DESARROLLO ECONÓMICO, SOCIAL, AMBIENTAL Y DE OBRAS PÚBLICAS DEL DISTRITO CAPITAL 2020-2024“UN NUEVO CONTRATO SOCIAL Y AMBIENTAL PARA LA BOGOTÁ DEL SIGLO XXI.* (11 de junio de 2020). Artículo 145. Agencia Analítica de Datos del Distrito.
- Aprobada en el Plan de Desarrollo, la Agencia Analítica de Datos. (6 de febrero de 2020). Alta Consejería Distrital TIC. Recuperado de: <https://tic.bogota.gov.co/node/1557>

- Akamai. (2019). State of the Internet - A year in review. Obtenido de <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/sotisecurity-a-year-in-review-report-2019.pdf>
- Departamento Nacional de Planeación. (2018, 17 de abril) Política Nacional de Explotación de Datos (Big Data) (Documento CONPES 3920). Bogotá D.C., Colombia: DNP.
- Departamento Nacional de Planeación. (2020, 01 de julio) Política Nacional de Confianza y Seguridad Digital (Documento CONPES 3995). Bogotá D.C., Colombia: DNP
- DNP. (2018). CONPES 3920. Obtenido de <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3920.pdf>
- Datereportal. (2020). DIGITAL 2020: PANORAMA DIGITAL GLOBAL. Obtenido de <https://datereportal.com/reports/digital-2020-global-digital-overview>
- McKinsey Global Institute. (2016). The age of analytics: Competing in a data-driven world. Obtenido de <https://www.mckinsey.com/~media/McKinsey/Industries/Public%20and%20Social%20Sector/Our%20Insights/The%20age%20of%20analytics%20Competing%20in%20a%20data%20driven%20world/MGI-The-Age-of-Analytics-Full-report.pdf>
- Mediana, E. (1 de junio de 2020). *Por qué y para qué sirve la Agencia Analítica de Datos aprobada en el Plan de Desarrollo*. Bogotá mi ciudad, Administración Distrital. Recuperado de: <https://bogota.gov.co/mi-ciudad/administracion-distrital/que-es-la-agencia-analitica-de-datos-de-la-alcaldia-de-bogota>
- National Cyber Security Index - NCSI. (7 de febrero de 2020). National Cyber Security Index. Obtenido de <https://ncsi.ega.ee/>
- Policía Nacional de Colombia. (2019, 29 de octubre) Informe de las tendencias del cibercrimen en Colombia (2019 – 2020). Primera Edición, Bogotá D.C., Colombia
- Sáenz, G. (14 de diciembre de 2020). Arranca Ágata, la nueva agencia de analítica de datos de Bogotá. Bogotá así vamos. Recuperado de: <https://bogota.gov.co/asi-vamos/gab/arranca-agata-la-nueva-agencia-de-analitica-de-datos-de-bogota>
- World Economic Forum. (2016). The 10 countries best prepared for the new digital economy. Obtenido de weforum.org: <https://www.weforum.org/agenda/2016/07/countries-best-prepared-for-the-newdigital-economy/>
- World Economic Forum. (19 de enero de 2016). World Economic Forum. Obtenido de World Economic Forum Global Agenda: <https://www.weforum.org/agenda/2016/01/what-is-the-fourth-industrialrevolution>
- Yohai. A.S. (2019) Prólogo. Informe de las tendencias del Cibercrimen en Colombia (2019 – 2020). Primera Edición, Bogotá D.C., Colombia.

7. IMPACTO FISCAL

De conformidad con lo anterior y en cumplimiento del artículo 7 de la Ley 819 de 2003, se aclara que el presente proyecto de acuerdo no genera un impacto fiscal que implique una modificación en el marco fiscal de mediano plazo, toda vez que estará encaminado a seguir los parámetros establecidos por la nueva Política Nacional de Explotación de Datos (Big Data), y el Plan de Desarrollo Distrital 2020 - 2024 “Un nuevo Contrato Social y Ambiental para el siglo XXI” en su propósito número 4 “Hacer de Bogotá - Región un modelo de movilidad multimodal, incluyente y sostenible” donde se busca aprovechar la inteligencia colectiva para hacer de Bogotá una ciudad que toma decisiones basadas en datos, información y evidencia, que aprovecha la tecnología y la transformación digital para el beneficio colectivo.

Cordialmente,

JUAN JAVIER BAENA MERLANO

Concejal de Bogotá

MARISOL GOMEZ GIRALDO

Concejal de Bogotá

CARLOS FERNANDO GALÁN PACHÓN

Concejal de Bogotá

Anexos: N/A

Copia: N/A

Elaboró: Ana María Pérez, Asesora; Juan Falkorneth, Asesor; Nicolás González, Pasante.

Revisó: Diana Parada, Asesora.

PROYECTO DE ACUERDO No. 439 DE 2020

PRIMER DEBATE

PROYECTO DE ACUERDO NO. DE 2020 “POR MEDIO DEL CUAL SE DICTAN LOS LINEAMIENTOS PARA LA PROMOCIÓN DEL CICLO VIRTUOSO DE LA SEGURIDAD, EL USO Y APROVECHAMIENTO DE LOS DATOS EN BOGOTÁ”.

EL CONCEJO DE BOGOTÁ, D. C.,

En ejercicio de sus atribuciones constitucionales y legales, en especial las conferidas en el artículo 12 del Decreto Ley 1421 de 1993,

ACUERDA:

Artículo 1. Objeto. La Administración Distrital en coordinación con las demás entidades pertinentes, establecerá una estrategia para la promoción del ciclo virtuoso de la seguridad, captura, uso, aprovechamiento y explotación de datos en Bogotá. Para estos cometidos institucionales, hará uso de las nuevas tecnologías y diseñará planes que permitan su implementación.

Artículo 2. Contrato Social sobre uso de datos. La Administración Distrital deberá diseñar un plan de trabajo acorde a la normatividad que rige la materia, con el fin de poner en funcionamiento un nuevo contrato social, que permita la democratización del uso de los datos para la construcción de ciudad inteligente, así como el fortalecimiento de las relaciones de confianza entre las personas y las entidades públicas. Para la creación del mismo, se realizarán mesas de trabajo por sectores económicos y de la Administración Distrital, con agremiaciones y sociedad civil, para poder articular en debida forma su participación y aporte en la materia.

Para la discusión y elaboración de un nuevo contrato social para el uso de datos, se propenderá por el empleo de tecnologías que maximicen su aprovechamiento, en particular, las emergentes y las pertenecientes a la cuarta revolución industrial. Así mismo, las que implementen la automatización, fomenten el uso de la inteligencia artificial, del internet de las cosas, basen sus predicciones en algoritmos y las demás que se consideren pertinentes para estos fines.

Artículo 3. Principios que deben regir en el uso de los datos. Entendiendo que la confianza, la integridad y la calidad de los datos son elementos esenciales para los fines públicos que se pretenden y para garantizar la privacidad de quien los aporta, se deberá observar y atender los siguientes principios, en concordancia con el marco normativo que desarrolla la materia en el país, especialmente, refiriendo a la Ley 1581 de 2012 y la Ley 1712 de 2014:

- a. Principio de transparencia. Los datos serán empleados para cometidos institucionales que vayan acorde con el interés general y colectivo, su uso se hará acorde a la ley, los principios generales del derecho y las buenas costumbres. Toda información y comunicación sobre los datos deberá ser clara y precisa.

- b. Principio de acceso de información. Al titular de la información se le permitirá el acceso a la información suministrada en todo momento, así como la posibilidad de hacer reclamos, modificarla y/o suprimirla.
- c. Principio de uso adecuado de datos. Se garantizará que los datos aportados únicamente se utilizarán para los fines estipulados y de requerirse algún cambio se pedirá consentimiento nuevamente.
- d. Principio de responsabilidad demostrada. Compromiso de la organización por incrementar sus estándares de protección para garantizar a las personas sus derechos como titulares.
- e. Principio de anonimización de los datos. Se velará por la privacidad de los datos personales y se anonimizarán cuando estos sean de uso abierto.

Artículo 4. Ética en el manejo de datos. Se debe adoptar y desarrollar una cultura sobre el uso responsable de datos para el ejercicio de los fines públicos, por tal razón, se respetarán los siguientes lineamientos, que en materia de datos serán de carácter obligatorio para todas las entidades del Distrito que capten, almacenen, administren, usen y exploten datos, entendiendo siempre que la confianza es el baluarte más importante en estos propósitos:

- a. Establecer claramente el fin y uso que se darán a los datos solicitados. No variar estos propósitos.
- b. Solicitar el consentimiento del titular de los datos para el uso que requiere la Administración Distrital. Usarlos únicamente para los fines mencionados y de tener que cambiar su uso volver a consultar a sus titulares.
- c. Adoptar todas las medidas de seguridad a que haya lugar con el fin de proteger la privacidad de la información.
- d. Darle la oportunidad a quien es dueño de los datos de modificarlos y suprimirlos en los casos que considere oportuno y necesario.

Artículo 5. Programa integral de Gestión de Datos personales. La Alta Consejería Distrital TIC, a través de la Comisión Distrital de Transformación Digital, orientará a todas las entidades del Distrito en la elaboración de programas integrales de gestión de datos personales, de conformidad con las necesidades y capacidades de cada una de ellas, con el propósito de que se implementen los controles necesarios para el tratamiento de la información personal y se administren los riesgos relativos a recolección y utilización de los datos.

Artículo 6. Calidad de los datos. La Administración Distrital junto a la Agencia Analítica de Datos, Ágata, o quien haga sus veces, apropiará y socializará los lineamientos del Gobierno Nacional, en los que se desarrollen aspectos relevantes sobre la calidad de los datos y su importancia para la construcción del ciclo virtuoso que se contempla en este acuerdo, así mismo, establecerá unos lineamientos mínimos para su completitud en los casos en que sea necesario y determinará los responsables en cada caso, en concordancia con el estándar universal de calidad de datos: disponibilidad, usabilidad, confiabilidad, relevancia y calidad de presentación.

Artículo 7. Evaluaciones de impacto de privacidad La Administración Distrital impartirá instrucciones a todas las entidades que la conforman, con el fin de que estas realicen anualmente y con corte a 31 de diciembre, evaluaciones del impacto de seguridad y de privacidad de la información antes de la recolección de los datos, durante su administración y posterior uso, proponiendo estrategias para reducir los impactos negativos e informando a los ciudadanos de las mismas oportunamente.

Se rendirá un informe anual sobre los resultados de las evaluaciones mencionadas y se allegaran al Concejo de Bogotá para su respectivo análisis y control, estos pueden ser los mismos que se presentan ante la Superintendencia de Industria y Comercio - SIC y las demás autoridades competentes.

Artículo 8. Sistemas de seguridad para los datos. La Administración Distrital deberá idear y poner en marcha un plan de trabajo en todas las entidades del Distrito Capital, para implementar tecnologías tradicionales y emergentes relativas a la seguridad y protección de datos, de acuerdo a las necesidades y capacidades de cada entidad, para los procesos de recolección, administración y uso de datos, con el fin de garantizar su seguridad, además de optimizar y modernizar su gestión.

Parágrafo único. Se propenderá por la ampliación del uso del Blockchain en las entidades públicas del orden Distrital, atendiendo los lineamientos que para estos fines dicte el Gobierno Nacional.

Artículo 9. Opacidad de los datos. En el caso en que la información sobre el tratamiento de los datos no sea clara, induzca a error o sea de difícil entendimiento para las personas titulares de los derechos, se adoptarán los correctivos necesarios para que, en virtud de la transparencia del uso de los datos, todas las personas puedan entender sus dinámicas y los fines que se persiguen con la utilización de estos. La información deberá ser comprensible para todas las personas respetando los diferentes niveles de entendimiento y capacidades. Esta se desarrollará concomitantemente con el derecho a conocer, de que trata la Ley 1581 de 2012 y demás normas que versen sobre la materia.

Artículo 10. Anonimización o seudonimización de los datos. La Administración Distrital realizará un protocolo de estricto cumplimiento para todas las entidades que estén a su cargo y trabajen con datos, en el cual se establezca la manera cómo se protegerá al titular de los datos y los procesos de anonimización o seudonimización en los casos que corresponda y cuando los mismos vayan a ser abiertos.

Parágrafo único. Cuando se esté frente a datos sensibles que pongan en riesgo la integridad de la persona, o vulnerar sus derechos fundamentales, el Distrito aplicará los protocolos adicionales que garanticen el anonimato de quienes aportan los datos.

Artículo 11. Aprovechamiento de datos no estructurados. La Administración Distrital promoverá al interior de sus entidades el aprovechamiento de información no estructurada, para la toma de decisiones basadas en datos y la posible explotación de los mismos, diseñando un plan de trabajo que permita establecer claramente el ciclo del dato.

Artículo 12. Oficial de Protección de Datos. La Administración Distrital creará el cargo de planta de Oficial de Protección de Datos en todas las entidades del Distrito, para que sea él quien esté encargado

de estructurar, diseñar y administrar las capacidades que le permitan a todas las entidades cumplir las normas sobre protección de datos personales, así como mitigar las vulnerabilidades asociadas a los mismos, en cumplimiento de los lineamientos establecidos por la Superintendencia de Industria y Comercio para tales fines.

Parágrafo único. En las entidades del Distrito Capital donde no sea posible crear el cargo de Oficial de Protección de Datos, por temas presupuestales, deberán entregar dichas responsabilidades a un funcionario de planta, incluyendo estas obligaciones en el manual de funciones en mención, mientras se logra crear formalmente el cargo. Esta medida será de naturaleza transitoria.

Artículo 13. Formación y educación continua en protección y aprovechamiento de datos. La administración Distrital deberá diseñar e implementar programas de capacitación que tengan por objeto dotar de capacidades a los servidores públicos sobre las obligaciones propias del régimen de protección de datos personales, así como también sobre herramientas para el uso, aprovechamiento y explotación de los datos para la gestión pública.

Estos procesos de formación serán extensivos a la ciudadanía en general, en los términos que determine la Administración Distrital.

Artículo 14. Vigencia. El presente Acuerdo rige a partir de la fecha de publicación.

PUBLÍQUESE Y CÚMPLASE

Anexos: N/A

Copia: N/A

Elaboró: Ana María Pérez, Asesora; Juan Falkorneth, Asesor; Nicolás González, Pasante.

Revisó: Diana Parada, Asesora.