



ALCALDÍA MAYOR
DE BOGOTÁ, D.C.

ACUERDO No. 002
(17 DIC 2025)

“Por el cual se adoptan lineamientos para la dinamización de la interoperabilidad en las entidades y organismos del Distrito Capital”

LA COMISIÓN DISTRITAL DE TRANSFORMACIÓN DIGITAL – CDTD

En ejercicio de sus funciones legales y reglamentarias, en especial las conferidas en el artículo 5, numeral 1 del Decreto Distrital 025 de 2021, el artículo 28 del Decreto Distrital 575 de 2023, y

CONSIDERANDO:

Que la Constitución Política de Colombia en su artículo 113 señala que los órganos del poder público deben colaborar armónicamente para el cumplimiento de los fines del Estado.

Que el artículo 16 del Decreto Ley 2150 de 1995, modificado por el artículo 14 de la Ley 962 de 2005, determina que, *“cuando las entidades de la Administración Pública requieran comprobar la existencia de alguna circunstancia necesaria para la solución de un procedimiento o petición de los particulares, que obre en otra entidad pública, procederán a solicitar a la entidad el envío de dicha información. En tal caso, la carga de la prueba no corresponderá al usuario. Será permitido el intercambio de información entre distintas entidades oficiales, en aplicación del principio de colaboración. (...)”*.

Que el Decreto 1078 de 2015, *“Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”*, en su Capítulo 1 del Título 9 de la Parte 2 del Libro 2, establece los lineamientos generales de la Política de Gobierno Digital, siendo los servicios ciudadanos digitales uno de sus habilitadores según lo señalado en el artículo 2.2.9.1.2.1.

Que este mismo Decreto en el numeral 1.1 del artículo 2.2.17.2.1.1 incluye dentro de los servicios ciudadanos digitales el servicio de interoperabilidad definido como aquél que *“(...) brinda las capacidades necesarias para garantizar el adecuado flujo de información e interacción entre los sistemas de información de las entidades, permitiendo el intercambio, la integración y la compartición de la información, con el propósito de facilitar el ejercicio de sus funciones constitucionales y legales, acorde con los lineamientos del marco de interoperabilidad. (...)”*.

Que el artículo 2.2.23.1.4. del Decreto referido anteriormente ordena a los sujetos obligados a la implementación de la política de gobierno a desarrollar iniciativas dinamizadoras de proyectos de Transformación Digital teniendo en cuenta, entre otros lineamientos y estándares, el de interoperabilidad, en virtud del cual dichos sujetos *“garantizarán la interoperabilidad entre los sistemas de información públicos para suministro e intercambio de la información de manera ágil y*



ALCALDÍA MAYOR
DE BOGOTÁ, D.C.

Continuación del Acuerdo No. 002 Página 2 de 6

“Por el cual se adoptan lineamientos para la dinamización de la interoperabilidad en las entidades y organismos del Distrito Capital”

eficiente conforme a los principios señalados en la Ley 1581 de 2012, o la norma que la modifique, adicione o sustituya. (...)”.

Que el Decreto 1083 de 2015, *“Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”* en el numeral 8 del artículo 2.2.35.3. establece que para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones (TIC), las entidades del Estado del orden nacional y territorial, los organismos autónomos y de control deberán *“adelantar acciones que faciliten la coordinación y articulación entre entidades del sector y del Estado en materia de integración e interoperabilidad de información y servicios, creando sinergias y optimizando los recursos para coadyuvar en la prestación de mejores servicios al ciudadano”*.

Que la Secretaría General de la Alcaldía Mayor de Bogotá, D.C., tiene entre sus funciones, según el artículo 2 del Decreto Distrital 140 de 2021 *“liderar, orientar y coordinar la política del sistema integral de información y su desarrollo tecnológico”*, lo cual hace necesario emitir los lineamientos que permitan la gestión y el intercambio eficiente de los datos distritales.

Que de conformidad con lo establecido en los numerales 1 y 3 del artículo 11 del Decreto Distrital 140 de 2021, corresponde a la Oficina Consejería Distrital de Tecnologías de la Información y las Comunicaciones - TIC expedir los lineamientos, directrices, estrategias e instrumentos para orientar la implementación y seguimiento de las políticas públicas de TIC y de gobierno digital del Distrito Capital.

Que el Decreto Distrital 575 de 2023 estableció la Infraestructura de Datos del Distrito Capital (IDD), definiendo la interoperabilidad como un componente esencial de dicha infraestructura y adoptando el Modelo Distrital de Gobernanza de Datos, con el objetivo de articular, orientar, y priorizar acciones para la generación, almacenamiento e intercambio de datos entre las instituciones distritales.

Que el artículo 28 de este mismo Decreto establece respecto de los lineamientos generales de interoperabilidad para el Distrito Capital, que *“los sujetos obligados aplicarán los lineamientos vigentes para el orden nacional, especialmente en lo relacionado con los servicios ciudadanos digitales, y para el orden distrital, los que expida la Comisión Distrital de Transformación Digital, o quien haga sus veces, en el marco del desarrollo de políticas, normativas, infraestructura tecnológica y lineamientos técnicos que permitan eliminar las barreras técnicas, institucionales y operativas para el intercambio de datos”*.

Que el artículo 228 del Acuerdo Distrital 927 de 2024 establece que la Secretaría General, a través de la Oficina Consejería Distrital de TIC, debe orientar y definir estrategias y acciones para impulsar la Transformación Digital y la implementación de proyectos estratégicos para la Ciudad Inteligente. De manera específica, el numeral 228.3 ordena *“promover el intercambio de datos en el*



ALCALDÍA MAYOR
DE BOGOTÁ, D.C.

Continuación del Acuerdo No. 002 Página 3 de 6

“Por el cual se adoptan lineamientos para la dinamización de la interoperabilidad en las entidades y organismos del Distrito Capital”

Distrito, para lo cual las entidades que hagan parte de los proyectos priorizados por el Comité Distrital de Datos deberán compartir los datos requeridos para casos de uso específico”.

Que este mismo Acuerdo establece mandatos expresos en diversos artículos (25, 207, 257 y 276) para el intercambio de información y la interoperabilidad en sistemas estratégicos (registro social de hogares, catastro, gestión documental y C4), lo cual requiere armonizar el cumplimiento de estos mandatos bajo un único marco de lineamientos técnicos y jurídicos.

Que el Acuerdo 001 de 2021 de la Comisión Distrital de Transformación Digital *“Por el cual se adopta el Reglamento Interno de la Comisión Distrital de Transformación Digital”* establece entre las funciones de esta Comisión, generar lineamientos en materia de transformación digital para el Distrito, en concordancia con los estándares que defina el Ministerio de TIC.

Que, en consecuencia, y para garantizar la observancia del principio constitucional de la función administrativa basado en la eficiencia, economía y celeridad, se hace indispensable expedir los lineamientos técnicos y jurídicos que deben observar las entidades y organismos del Distrito Capital para el intercambio efectivo de datos y la garantía de la interoperabilidad de sus sistemas de información, en coherencia con el marco normativo nacional y distrital.

Que en sesión ordinaria adelantada el 27 de octubre de 2025, la Comisión Distrital de Transformación Digital, en cumplimiento de sus funciones aprobó el presente Acuerdo, según consta en el Acta No. 03 de 2025.

En mérito de lo expuesto, la Comisión Distrital de Transformación Digital,

ACUERDA:

Artículo 1. Objeto: Adoptar los lineamientos y directrices que orienten y faciliten la implementación de mecanismos y acciones para la dinamización de la interoperabilidad entre las entidades y organismos del Distrito Capital, con el fin de promover el intercambio eficiente, ágil, seguro y oportuno de información.

Las entidades y organismos distritales deberán cumplir con los lineamientos, mejores prácticas y estándares técnicos de este acuerdo y sus anexos, las cuales servirán de orientación y estandarización para todos los actores involucrados en el proceso de interoperabilidad.

Artículo 2. Definiciones. Se adoptan como referentes las siguientes definiciones:

Acuerdo de intercambio: Es el documento formal que se establece y firma entre entidades y organismos públicos y privados para habilitar el intercambio de datos e interoperar entre sus sistemas de información. El acuerdo de intercambio establece el objeto, plazo de ejecución, especificaciones técnicas, obligaciones, derechos de las partes, entre otros.



ALCALDÍA MAYOR
DE BOGOTÁ, D.C.

Continuación del Acuerdo No. 002 Página 4 de 6

“Por el cual se adoptan lineamientos para la dinamización de la interoperabilidad en las entidades y organismos del Distrito Capital”

Interfaz de Programación de Aplicación - API (por sus siglas en inglés *Application Program Interface*): Son servicios web e interfaces basadas en estándares que permiten a las aplicaciones de software y sistemas de información exponer sus funcionalidades a sistemas externos. Las API definen cómo interactúa una aplicación con otra, de forma estructurada para facilitar la integración y el intercambio de datos.

Artículo 3. Lineamientos de interoperabilidad. Los lineamientos y directrices de interoperabilidad están agrupados por los dominios establecidos en el Marco de Interoperabilidad del Estado definido por el Ministerio de TIC.

3.1 Dominio Político – Legal

a) Acuerdos de intercambio de datos

A partir de la expedición de este acuerdo, las entidades y organismos distritales deberán asegurar la interoperabilidad de sus sistemas de información, disponiendo para ello de los recursos humanos, físicos, tecnológicos, técnicos y financieros necesarios. Para lograrlo, en adelante, deberán establecer y firmar acuerdos de intercambio de datos, utilizando los formatos definidos en el Anexo 1 Plantilla Acuerdo de Confidencialidad e Intercambio de Información celebrado entre entidades, y en el Anexo 2 Anexo Técnico de este acuerdo. Las entidades podrán editar, eliminar o complementando la información de estos formatos, según cada caso.

El plazo máximo para la estructuración y firma de estos acuerdos será de noventa (90) días calendario a partir de la recepción de la solicitud de intercambio.

3.2 Dominio Organizacional

a) Rol de Administrador de datos como dinamizador de la interoperabilidad

Todas las entidades distritales deberán designar el rol de administrador de datos conforme a lo establecido en el Título 24 a la Parte 2 del Libro 2 del Decreto 1078 de 2015 del Ministerio de TIC y en el marco de las funciones definidas en el Decreto Distrital 575 de 2023. Este rol será el responsable de liderar, articular y dinamizar las acciones relacionadas con la interoperabilidad de datos en la entidad, en coordinación con la Oficina Consejería Distrital de TIC y el Comité Distrital de Datos.

Parágrafo: La designación de este rol se deberá realizar de conformidad con lo dispuesto en el Anexo 3 de este acuerdo, Perfil del administrador de datos.

b) Esquema de gobernanza de la interoperabilidad



ALCALDÍA MAYOR
DE BOGOTÁ, D.C.

Continuación del Acuerdo No. 002 Página 5 de 6

“Por el cual se adoptan lineamientos para la dinamización de la interoperabilidad en las entidades y organismos del Distrito Capital”

Las entidades distritales deberán adoptar el Anexo 4 Esquema de gobierno de interoperabilidad como parte del Modelo de Gobernanza de Infraestructura de Datos del Distrito.

3.3 Dominio Técnico

a) Diseño de aplicaciones, trámites y servicios basados en API.

Todas soluciones y aplicaciones de software o sistemas de información que se desarrollen en las entidades y organismos públicos distritales deberán ser diseñadas y desarrolladas bajo arquitecturas basadas en servicios y API y proveer una API de conexión segura para la exposición de datos.

b) Estandarización de API y servicios web.

Todas las API que se desarrollen en las entidades y organismos distritales deberán seguir los lineamientos y especificaciones técnicas para el diseño de API y servicios web distritales definidos en el Anexo 5 Lineamientos y especificaciones técnicas para el diseño de API's y servicios web distritales.

c) Publicación en el repositorio de API y servicios del distrito.

Todas las API que se desarrollen y se actualicen en las entidades del Distrito para el intercambio de datos e interoperabilidad deben publicarse en el repositorio de API y servicios del Distrito.

d) Plataformas de intercambio de datos e interoperabilidad.

De acuerdo con el nivel de madurez de las entidades del Distrito para el intercambio de datos, el volumen de datos y la variabilidad de los datos, cada entidad definirá el canal y la plataforma de intercambio de datos e información inicial más adecuada y deberá evolucionar de manera gradual hasta mejorar su nivel de madurez.

3.4 Dominio Semántico

a) Registro en el catálogo de datos distritales.

Todas las entidades del distrito deben registrar el 100% de sus fuentes de información y datos en el catálogo de datos distritales que disponga la Oficina Consejería TIC y mantenerlos actualizados.

b) Registro de fuentes de información y registros administrativos.

Todas las entidades y organismos distritales deberán registrar el 100% de sus fuentes de información y registros administrativos en el Sistema de Identificación y Caracterización de Oferta y Demanda Estadística (SICODE) del Departamento Administrativo Nacional de Estadística



ALCALDÍA MAYOR
DE BOGOTÁ, D.C.

Continuación del Acuerdo No. 002 Página 6 de 6

“Por el cual se adoptan lineamientos para la dinamización de la interoperabilidad en las entidades y organismos del Distrito Capital”

(DANE) y mantenerlos actualizados de acuerdo con la Ley 2335 de 2023 o la norma que lo modifique, sustituya o adicione.

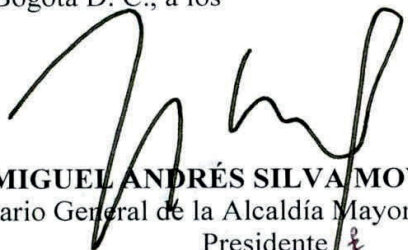
Parágrafo: Para avanzar y contar con la totalidad de los registros administrativos de las entidades distritales registrados y actualizados en el SICODE, se establecerá la priorización de los registros administrativos del Distrito Capital.

Artículo 4. Vigencia y derogatoria. El presente Acuerdo rige a partir del día siguiente a la fecha de su publicación, y deroga las disposiciones que le sean contrarias.

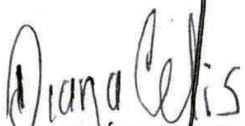
PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE

Dado en Bogotá D. C., a los

17 DIC 2025


MIGUEL ANDRÉS SILVA MOYANO

Secretario General de la Alcaldía Mayor de Bogotá D.C.
Presidente


DIANA ROCÍO CELIS MORA

Jefe de la Oficina Consejería Distrital de Tecnologías de la Información y las Comunicaciones – TIC, Secretaría General de la Alcaldía Mayor de Bogotá D.C.
Secretaria Técnica

Proyectó: Felipe Valencia – Asesor, Secretaría General de la Alcaldía Mayor de Bogotá D.C.
Revisó: Adriana Martínez – Asesora Oficina Consejería Distrital de TIC

ANEXO 1
PLANTILLA ACUERDO DE CONFIDENCIALIDAD E INTERCAMBIO DE
INFORMACIÓN CELEBRADO ENTRE ENTIDADES

Entre los suscritos a saber, por una parte, la ENTIDAD 1 que para los efectos del presente acuerdo se encuentra representada por [Nombres y Apellidos del(a) representante de la ENTIDAD 1], identificado(a) con cédula de ciudadanía (C.C.) [Número de c.c. del(a) representante de la ENTIDAD 1], en su calidad de [Cargo del(a) representante de la ENTIDAD 1] y nombrado(a) mediante resolución [Número y año de la resolución de nombramiento del(a) representante de la ENTIDAD 1], y por la otra parte la ENTIDAD 2, representada para efectos del presente acuerdo por [Nombres y Apellidos del(a) representante de la ENTIDAD 2] identificado(a) con la C.C. [Número de c.c. del(a) representante de la ENTIDAD 2], en su calidad de [Cargo del(a) representante ENTIDAD 2] nombrado(a) mediante resolución [Número y año de la resolución de nombramiento del(a) representante de la ENTIDAD 2]. Ambas entidades con autonomía administrativa y financiera, hemos convenido celebrar el presente ACUERDO DE CONFIDENCIALIDAD E INTERCAMBIO DE INFORMACIÓN en los siguientes términos y condiciones:

CONSIDERACIONES

Considerando lo siguiente:

1. Que, dentro de los fines esenciales del Estado, determinados en el artículo 2 de la Constitución Política de Colombia, se encuentra el “(...) *servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes* (...)”. Así mismo, el artículo 113 de la misma, establece el principio de colaboración armónica entre los diferentes órganos del Estado. Igualmente, el artículo 209 de la Carta Política, consagra que la función administrativa debe estar al servicio de los intereses generales y desarrollarlos con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones. Es por ello que las autoridades administrativas deben coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado.

2. Que el artículo 5 de la Ley 489 de 1998, establece que los organismos administrativos ejercerán con exclusividad las potestades y atribuciones inherentes, de manera directa e inmediata, respecto de los asuntos que les hayan sido asignados expresamente por la ley, la ordenanza, el acuerdo o el reglamento ejecutivo, entendiéndose que los principios de la función administrativa y los principios de coordinación, concurrencia y subsidiariedad consagrados por el artículo 288 de la Constitución Política, deben ser observados en el señalamiento de las competencias propias de los organismos y entidades de la rama ejecutiva y en el ejercicio de las funciones de los servidores públicos.

Aunado a lo anterior, el artículo 6 de la Ley 489 de 1998, consagra que “*En virtud del principio de coordinación y colaboración, las autoridades administrativas deben garantizar la armonía en el ejercicio de sus respectivas funciones con el fin de lograr los fines y cometidos estatales. En consecuencia, prestarán su colaboración a las demás entidades para facilitar el ejercicio de sus funciones y se abstendrán de impedir o estorbar su cumplimiento por los órganos, dependencias, organismos y entidades titulares*”.

Adicionalmente, el artículo 95 ibídem establece que las entidades públicas podrán asociarse con el fin de cooperar en el cumplimiento de funciones administrativas o de prestar conjuntamente servicios que se hallen a su cargo, mediante la celebración de convenios interadministrativos.

3. Que, respecto al intercambio de información, la Ley 2335 de 2023, establece en su artículo 17 sobre Intercambio de información estadística que, *“quienes conforman el Sistema Estadístico Nacional - SEN, podrán intercambiar información estadística correspondiente a datos agregados y a microdatos de forma gratuita y oportuna en desarrollo de los objetivos del SEN, en los términos del artículo 27 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo y demás normas concordantes, así como de las Leyes Estatutarias 1266 de 2008 y 1581 de 2012 y las normas que las modifiquen o sustituyan”*.

5. Que el Artículo 3 del Decreto 235 de 2010, modificado por el Artículo 1 del Decreto 2280 de 2010, establece que *“(...) para efectos de formalizar el intercambio de información de manera ágil, oportuna y confiable, las entidades públicas o los particulares encargados de una función administrativa podrán emplear el mecanismo que consideren idóneo para el efecto, tales como cronograma de entrega, plan de trabajo, protocolo o convenio, entre otros (...)”*.

6. A su turno, el artículo 159 de la Ley 1753 de 2015 modificadorio del artículo 227 de la Ley 1450 de 2011, establece la obligatoriedad de suministro de información, así:

“Para el desarrollo de los planes, programas y proyectos incluidos en el Plan Nacional de Desarrollo y en general para el ejercicio de las funciones públicas, las entidades públicas y los particulares que ejerzan funciones públicas pondrán a disposición de las entidades públicas que así lo soliciten, la información que generen, obtengan, adquieran o controlen y administren, en cumplimiento y ejercicio de su objeto misional. El uso y reutilización de esta información deberá garantizar 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, así como las demás normas que regulan la materia.

El suministro de la información será gratuito, deberá solicitarse y realizarse respaldado en estándares que faciliten el proceso de intercambio y no en tecnologías específicas que impidan el acceso, no estará sujeto al pago de tributo, tarifa o precio alguno y las entidades públicas solo podrán cobrar los costos asociados a su reproducción o los derivados de la aplicación de procesamientos o filtros especiales. Las entidades públicas propenderán por la integración de los sistemas de información para el ejercicio eficiente y adecuado de la función pública. (...)”

8. Que la Administración Distrital necesita mejorar la calidad de la información que administra relacionada con la ciudadanía, con el fin de optimizar los sistemas de información, lo cual permitirá hacer más eficiente el acceso a información, trámites y servicios que se requieran.

9. En relación con la información de las personas y en general en cuanto a los temas de la identificación ciudadana, la normatividad vigente es restrictiva, dada la naturaleza de la información, según lo establecido en la Ley Estatutaria 1581 de 2012, *“Por la cual se dictan disposiciones generales para la protección de datos personales”*, reglamentada parcialmente por el Decreto Nacional 1074 de 2015 en el capítulo 25 artículo 2.2.2.25.1.2 que establece que para el tratamiento de los datos de carácter personal se debe contar con autorización previa, expresa e informada del titular. No obstante, en el artículo 10 de la citada Ley, dispone que la autorización de tratamiento de datos personales por el Titular no será necesaria cuando se trate de: *“a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales (...)”*. Sin embargo, quien

acceda a los datos personales sin que medie autorización previa deberá en todo caso, cumplir con las disposiciones contenidas en la Ley 1581 de 2012.

10. De acuerdo con lo anteriormente expuesto y para el cumplimiento de los fines antes descritos, se requiere la colaboración oportuna y decidida de todas las instituciones públicas que estén en condiciones de proveer información para robustecer la calidad de los datos del Distrito Capital, así como establecer el mecanismo para el intercambio de información catalogada como reservada o confidencial y que soliciten las entidades en cumplimiento de sus objetos misionales.

En mérito de lo expuesto, se suscribe el presente acuerdo de confidencialidad el cual se regirá por las siguientes cláusulas:

1. PARTES DEL ACUERDO

Las partes declaran que para el presente acuerdo serán al tiempo reveladoras y receptoras, por tanto, el mismo se aplica en el sentido que corresponda, de acuerdo con la información confidencial tratada.

A. OBJETO DEL ACUERDO:

Aunar esfuerzos entre la ENTIDAD 1 y la ENTIDAD 2, para intercambiar datos e interoperar entre las partes, que favorezca el cumplimiento de las funciones misionales, conforme a las condiciones pactadas en el presente Acuerdo de Confidencialidad e Intercambio de Información y el Anexo Técnico que hace parte integral del mismo.

B. PRINCIPIOS:

Con el objeto de cumplir los propósitos del presente Acuerdo de Confidencialidad e Intercambio de Información, las partes se comprometen a actuar de conformidad con los siguientes principios:

1. Colaboración: LAS PARTES prestarán asistencia y ayuda mutua a través de los mecanismos tecnológicos y técnicos y del factor humano con el que cuentan para el desarrollo de las actividades propias de este convenio y cualquiera otras que se deriven de su ejecución, previamente definidas de acuerdo con los mecanismos establecidos en el presente convenio y en concordancia con las funciones y competencias de cada parte.

2. Confidencialidad: Según el cual es obligación de LAS PARTES guardar absoluta y total reserva respecto de la información, medios y herramientas interactuante entre ellas, con el único y exclusivo fin de ser utilizada en ejercicio de sus competencias y funciones, para lo cual deberán ejercer las acciones pertinentes relativas a evitar la pérdida, destrucción, alteración, acceso y uso no autorizado o fraudulento de la información.

3. Seguridad: Según el cual, para todos los casos, LAS PARTES deben adoptar todas las medidas necesarias desde el punto de vista técnico de hardware, software, comunicaciones, redes e instalaciones físicas, procedimientos y personal, para garantizar la custodia debida de la información, herramientas y/o sistemas y su consecuente uso conforme a los fines del presente Acuerdo de Confidencialidad e Intercambio de Información, de conformidad con las competencias que corresponden a cada una de éstas.

4. Pertinencia y consecuencia: Según el cual LAS PARTES del presente Acuerdo de Confidencialidad e Intercambio de Información asienten en hacer uso exclusivo y restringido de la información interactuante y herramientas tecnológicas interactuantes, conforme a las competencias

que por Ley se han definido a cargo de cada una de ellas, sin perjuicio de iniciar las acciones correspondientes cuando se verifique el mal uso de la información o herramientas, su pérdida, deterioro, destrucción o alteración o cualquier otra conducta que entrañe un indebido uso o aplicación de la información. Dichas acciones podrán ser administrativas, disciplinarias y penales según corresponda.

PARÁGRAFO: La información compartida sólo podrá ser utilizada para los efectos del presente Acuerdo de Confidencialidad e Intercambio de Información y no podrá ser utilizada para fines comerciales o de explotación económica por ninguna de LAS PARTES. Tampoco podrá ser entregada a entidades públicas o privadas de carácter nacional o internacional, sin la autorización previa de la entidad 1 o 2 según corresponda y la suscripción del acuerdo de confidencialidad establecido por la ENTIDAD 1 y la ENTIDAD 2 y los respectivos acuerdos de intercambio de información suscritos entre la ENTIDAD 1 y la ENTIDAD 2.

2. COMPROMISOS DE LAS PARTES

2.1. Compromisos Generales:

Las PARTES del presente Acuerdo de Confidencialidad e Intercambio de Información son las únicas destinatarias de la información que se entregue en desarrollo de este, para lo cual se comprometen a:

1. Ejecutar idónea y oportunamente el objeto del presente Acuerdo de Confidencialidad e Intercambio de Información.
2. Poner a disposición, según disponibilidad, las herramientas informáticas requeridas para el desarrollo del presente Acuerdo de Confidencialidad e Intercambio de Información.
3. Facilitar el acceso e intercambio de la información que se requiera en desarrollo del presente Acuerdo de Confidencialidad e Intercambio de Información, respetando las normas de habeas data y protección de datos personales que resulten aplicables a este.
4. Suministrar la información contenida en los anexos técnicos durante la vigencia del acuerdo.
5. Garantizar que los datos intercambiados no sean utilizados para fines diferentes a los aquí expuestos. Para estos efectos, no se considera un uso ilegítimo de la información cuando los datos intercambiados sean transformados, modificados o adicionados a otros datos con los que cuenten.
6. Suministrar al Supervisor del Acuerdo, las credenciales de acceso para la consulta de la información.
7. Realizar por parte de cada entidad (tanto la que entrega como la que recibe la información del presente acuerdo) la capacitación necesaria a los funcionarios y/o contratistas designados, por las partes sobre el manejo del sistema e interpretación de la información y los reportes y las modificaciones del sistema de información. Igualmente, proveer los manuales diseñados para tales efectos.
8. Guardar reserva y confidencialidad de la información a que tenga acceso en desarrollo del acuerdo en virtud de la cláusula séptima y procurar los medios necesarios a fin de evitar los riesgos de pérdida, destrucción, alteración y uso no autorizado o fraudulento de la información a la que tenga acceso en desarrollo del acuerdo.
9. Suministrar cuando lo requiera, los informes necesarios que permitan dar respuesta a solicitudes elevadas por autoridades, relacionadas con el objeto del acuerdo.
10. Permitir incorporar a sus bases de datos, la información resultante del intercambio de información objeto del presente Acuerdo de Confidencialidad e Intercambio de Información, con fines estadísticos.
11. Informar oportunamente a las partes cualquier sugerencia para el mejoramiento del Acuerdo de Confidencialidad e Intercambio de Información o anomalía en la ejecución del mismo.

2.2. Compromisos Específicos de las partes:

1. LAS PARTES deberán mantener en confidencialidad la información recibida y no revelarla total o parcialmente, a ninguna persona diferente al personal que necesite conocerla en relación con los términos y condiciones del presente Acuerdo de Confidencialidad e Intercambio de Información. Para revelar la información deberá existir consentimiento previo por escrito por LAS PARTES.
2. LAS PARTES utilizarán la información que reciba, únicamente en los temas que se desarrollen en el contexto del presente Acuerdo de Confidencialidad e Intercambio de Información. En ningún caso la información podrá ser utilizada con propósitos que perjudiquen o causen detrimento a la otra parte.
3. Ninguna de LAS PARTES revelará o autorizará a sus funcionarios y/o contratistas, compartir la información revelada con terceros, salvo que cuente con el consentimiento previo y escrito de la otra parte.
4. LAS PARTES declaran que cuentan con las autorizaciones legales o de los titulares para entregar la información objeto de intercambio.
5. LAS PARTES deberán tomar las medidas de seguridad que sean necesarias y razonables, para que sus servidores, técnicos, consultores, contratistas y colaboradores, que tengan acceso a la información confidencial intercambiada, actúen en cumplimiento del deber de confidencialidad de este acuerdo. LAS PARTES serán responsables por el incumplimiento de las obligaciones de sus funcionarios, técnicos, consultores, contratistas y colaboradores en los términos del presente Acuerdo.
6. No comercializar, duplicar total o parcialmente, en medios propios o ajenos, magnéticos o de cualquier tipo, tanto el software, como la información contenida en las bases de datos que se intercambien, o desarrollar a partir de la información proporcionada productos o servicios en beneficio de terceros, utilizando la información y en general formulas, algoritmos, o procedimientos inherentes a cada entidad. No utilizar la información de la otra entidad de manera total o parcial, mediante el uso de bases de información, software o aplicativos internos en beneficio de terceros, para actividades que no estén relacionadas con el presente acuerdo y que no hayan sido autorizadas de manera previa por la parte titular de la propiedad de la información de los bienes de propiedad intelectual.
7. LAS PARTES deberán entregar y/o suministrar la información confidencial únicamente a la(s) persona(s) autorizada(s) e identificada(s) expresamente en las actas de reunión que se lleven a cabo en virtud del desarrollo del presente Acuerdo de Confidencialidad e Intercambio de Información, de acuerdo con el anexo técnico y que hace parte integral de este.
8. Si una de LAS PARTES extravía o revela información confidencial, dará aviso inmediato a la otra y tomará todas las medidas razonables y necesarias para minimizar los resultados de la pérdida de la información extraviada o divulgada sin autorización.
9. LAS PARTES no serán responsables cuando la pérdida o extravío de la información se origine como consecuencia de fuerza mayor o caso fortuito.

3. INFORMACIÓN CONFIDENCIAL

La información transmitida en forma previa o posterior a este Acuerdo de Confidencialidad e Intercambio de Información por LAS PARTES, a excepción de aquellos datos de naturaleza pública, tiene carácter de confidencial. Esta información puede incluir información pública clasificada, información pública reservada, además de información técnica, financiera, estratégica y cualquier información relacionada con las operaciones presentes y futuras de LAS PARTES, la cual puede transmitirse en forma escrita, oral o visual. La información generada en el marco del ejercicio de las funciones administrativas y de los objetivos misionales que legalmente les han sido otorgadas a cada

una de las partes también es considerada confidencial, salvo que se trate de datos considerados públicos conforme a lo dispuesto en el numeral 2, del artículo 2.2.2.25.1.3 Decreto 1074 de 2015.

4. INFORMACIÓN OBJETO DEL INTERCAMBIO

Las especificaciones técnicas relativas a la ejecución del presente Acuerdo de Confidencialidad e Intercambio de Información se desarrollan a través del Anexo Técnico el cual debe incluir la información que será objeto de entrega o intercambio, así como los mecanismos tecnológicos, infraestructura y procedimientos que deberán ser utilizados y aplicados. El Anexo Técnico podrá tener ajustes a la luz de los cambios que tengan los diccionarios de las bases compartidas u otro tema relacionado con los mecanismos definidos.

Para lograr la calidad de la información que suministra y utiliza en forma adecuada, LAS PARTES deberán dar estricta aplicación a los documentos técnicos que se suscriban en el marco del presente Acuerdo de Confidencialidad e Intercambio de Información.

LAS PARTES se comprometen a entregar la información solicitada en la periodicidad requerida a través de los mecanismos, herramientas y procedimientos acordados, sin que ello desborde el alcance de la normatividad vigente en la materia, en los términos establecidos en los Anexos Técnicos correspondientes.

5. CONDICIONES DE CUSTODIA DE LA INFORMACIÓN

LAS PARTES custodiarán la información recibida y se comprometen a aplicar todas las medidas de seguridad necesarias para preservarla en términos de confidencialidad, integridad y disponibilidad. Para efectos de lo anterior aplicarán medidas para evitar la divulgación, fuga, modificación o uso no autorizado de la información recibida. Adicionalmente, se conviene que toda la información sea guardada en un lugar con acceso limitado únicamente a las personas que la utilizan y requieran conocerla en desarrollo de sus obligaciones y de la misma forma se deberán adoptar las medidas necesarias para evitar dañar o contaminar la información transmitida.

6. HABEAS DATA

Las partes reconocen que en desarrollo del Acuerdo de Confidencialidad e Intercambio de Información pueden llegar a tener acceso a información de carácter privado o reservado por el derecho fundamental del Habeas Data, establecido en el artículo 15 de la Constitución Política de Colombia, en la Ley 1581 de 2012 y los Decretos 1074 de 2015 de y 1081 de 2015. Por consiguiente, las partes se obligan a manipular esta información de carácter privado o reservado con sujeción a las normas y disposiciones constitucionales y/o legales y vigentes, y a la jurisprudencia de la Corte Constitucional sobre la materia. Adicionalmente, LAS PARTES no podrán disponer de bases de datos individuales a entidades públicas o privadas diferentes a las intervinientes en este Acuerdo.

7. DERECHOS PROPIEDAD INTELECTUAL

La entrega de información sea confidencial o no, no concede autorización, permiso o licencia de uso de marcas comerciales, patentes, derechos de autor o de cualquier otro derecho de propiedad industrial o intelectual. La entrega o recepción de información no constituirá o implicará promesa de efectuar contrato posterior alguno por cualquiera de LAS PARTES.

En consecuencia, LAS PARTES no podrán modificar, copiar o elaborar productos, sistemas, modelos, diseños, planos, y demás creaciones intelectuales provistos bajo este acuerdo; en caso de necesitar usar la propiedad intelectual LAS PARTES, deberán solicitar autorización previa expresa y escrita.

8. DERECHOS DE AUTOR

Todos los documentos y productos que las partes desarrollen en ejecución del presente Acuerdo de Confidencialidad e Intercambio de Información, incluidos los derechos patrimoniales de autor, serán de propiedad exclusiva de la productora.

9. CAUSALES DE TERMINACIÓN

Son causales de terminación del presente Acuerdo, las siguientes: 1) Por violación comprobada de la confidencialidad o reserva de la información que debe observar cada una de LAS PARTES, sin perjuicio de las acciones legales a que haya lugar por este hecho. 2) En forma anticipada por mutuo Acuerdo entre LAS PARTES, para lo cual la parte interesada deberá enviar comunicación sobre el particular a la otra, con una anticipación no inferior a noventa (90) días. 3) Por expiración del plazo pactado.

PARÁGRAFO: En caso de terminación del presente Acuerdo, LAS PARTES devolverán todos los originales, copias, reproducciones y resúmenes de la información confidencial a pedido de LAS PARTES, y certificarán la destrucción de la misma salvo aquella información que fue empleada para el desarrollo de modelos estadísticos o de riesgo, teniendo en cuenta la imposibilidad de identificar de manera individual la información revelada.

10. DURACIÓN DEL ACUERDO

La duración del presente acuerdo es de tres (3) años contados a partir de la suscripción del mismo. Este plazo podrá ser prorrogado por acuerdo entre LAS PARTES, mediante documento debidamente suscrito por los representantes legales, siempre que dentro de los sesenta (60) días calendario anteriores a su vencimiento, los supervisores manifiesten por escrito el interés y la necesidad de su prórroga.

11. PROHIBICION DE CESION

Este Acuerdo de Confidencialidad e Intercambio de Información debe beneficiar y comprometer a LAS PARTES y no puede ser cedido, asignado, ni transferido bajo ninguna forma y a ningún título, sin contar con la autorización previa y escrita de la otra parte.

12. INDEMNIDAD

LAS PARTES se mantendrán indemnes entre sí por las consecuencias que resulten de las actuaciones de sus funcionarios o de terceros contratados por ellas, con ocasión a la ejecución del presente acuerdo. En este sentido cada una asumirá la responsabilidad por el manejo de la información suministrada en desarrollo de este acuerdo y responderá civil y penalmente, tanto por el incumplimiento de las obligaciones imputables y que causen daño y/o perjuicio a la entidad, derivados de la celebración y ejecución del mismo.

Cada una de LAS PARTES asumirá la responsabilidad por el manejo y uso de la información suministrada en desarrollo de este acuerdo y responderá legalmente tanto por el incumplimiento de

los compromisos derivados del mismo, como por los hechos u omisiones que le fueran imputables y que causen daño y/o perjuicio a la Entidad o terceros, derivados de la celebración y ejecución de este Acuerdo.

13. SUSPENSIÓN

De común acuerdo las intervinientes podrán suspender la ejecución de este Acuerdo, por circunstancias tales como: a) Necesidades del servicio, b) Razones de fuerza mayor o caso fortuito. Caso en el cual suscribirán un acta donde se hará constar tal situación.

14. GRATUIDAD

El presente Acuerdo de Confidencialidad e Intercambio de Información no tiene valor económico. No habrá remuneración pecuniaria entre las partes que lo suscriban. Los gastos que impliquen el cumplimiento de sus obligaciones serán sufragados por la parte que deba cumplirlas con cargo a su respectivo presupuesto.

15. SUPERVISIÓN:

La supervisión del cumplimiento del presente Acuerdo de Confidencialidad e Intercambio de Información estará a cargo de:

Por la ENTIDAD 1:

La supervisión será ejercida por [Nombres y Apellidos del(a) representante de la ENTIDAD 1] de [Nombre de la dependencia de la ENTIDAD 1 a la que pertenece].

Por la ENTIDAD 2

La supervisión será ejercida por [Nombres y Apellidos del(a) representante de la ENTIDAD 2] de [Nombre de la dependencia de la ENTIDAD 2].

PARÁGRAFO: La supervisión hará por escrito todas las observaciones y sugerencias que considere necesarias para el cabal desarrollo del objeto del Acuerdo de Confidencialidad e Intercambio de Información y el cumplimiento de los compromisos de las partes.

16. MODIFICACIÓN

Este Acuerdo de Confidencialidad e Intercambio de Información solo podrá ser modificado con el consentimiento expreso por escrito de ambas partes.

17. SOLUCIÓN DE CONTROVERSIAS:

LAS PARTES acuerdan que, en el evento de suscitarse cualquier controversia en relación con la ejecución del presente Acuerdo de Confidencialidad e Intercambio de Información, las mismas serán resueltas mediante procedimientos directos de solución de conflictos como la negociación directa, la transacción de la conciliación o la amigable composición, sin desconocer otros mecanismos establecidos en las leyes colombianas vigentes.

18. INHABILIDADES E INCOMPATIBILIDADES.

LAS PARTES declaran bajo la gravedad del juramento que no se hayan incurrido en causal alguna de inhabilidad e incompatibilidad establecida en la Constitución Política y en la Ley.

19. PERFECCIONAMIENTO Y EJECUCIÓN.

El presente Acuerdo de Confidencialidad e Intercambio de Información requiere para su perfeccionamiento y ejecución la firma de las partes.

20. NOTIFICACIONES

Para efectos de las comunicaciones que se deban surtir entre las partes de este Acuerdo, referentes al cumplimiento de sus obligaciones, se acuerdan las siguientes direcciones y teléfonos: *(se recomienda que sea el administrador de datos de cada entidad o funcionarios de planta.)*

ENTIDAD 1

Nombres y Apellidos:
Correo electrónico: xxx@xxx.gov.co
Dirección:
Teléfono:

ENTIDAD 2

Nombres y Apellidos:
Correo electrónico: xxx@xxx.gov.co
Dirección:
Teléfono:

El presente documento se firma a los [NÚMERO DEL DÍA] días del mes de [NOMBRE DEL MES] de [NÚMERO DEL AÑO].

Las partes,

POR LA ENTIDAD 1
Nombre del representante
Cargo

POR LA ENTIDAD 2
Nombre del representante
Cargo

ANEXO 2

ANEXO TÉCNICO

Este Anexo Técnico hace parte integral del Acuerdo de Confidencialidad e Intercambio de Información suscrito entre ENTIDAD 1 y LA ENTIDAD firmado el día [XX] del mes de [XX] del año [XX], dando cumplimiento a los artículos 2.1, 2.2 y 4 del citado Acuerdo.

Tiene como objetivo especificar las características técnicas, mínimos semánticos de la información que será compartida entre las partes, los diccionarios de datos, los mecanismos que se usarán y las consideraciones adicionales sobre seguridad, protección de datos y acuerdos de niveles de servicio que se tendrán en cuenta durante el proceso de intercambio.

Las dependencias encargadas de la transferencia de la información del Acuerdo de Confidencialidad e Intercambio de Información deberán ejecutar y realizar seguimiento a los compromisos adquiridos en el presente documento, por lo que debe:

Disponer los datos de acuerdo con la periodicidad de intercambio de información acordados en el presente documento

Generar las alertas oportunamente cuando las fuentes de información o herramientas presenten alguna modificación o no se puedan disponer en los tiempos pactados,

Gestionar y administrar la asignación de usuarios para el acceso a la información

Gestionar las acciones necesarias a fin de garantizar la efectividad de los procesos de intercambio de información e interoperabilidad.

Definir los acuerdos de Nivel de servicio para el intercambio de datos e interoperabilidad.

Las entidades firmantes del Acuerdo de Confidencialidad e Intercambio de Información acuerdan compartir los siguientes registros administrativos de programas o fuentes de información para el ejercicio misional de las partes:

Bases de Datos	Por la Entidad 1	Por la Entidad 2
[Base de datos 1]	[Nombre del registro o base de datos]	[Nombre del registro o base de datos]
[Base de datos 2]	[Nombre del registro o base de datos]	[Nombre del registro o base de datos]
[Base de datos 3]	[Nombre del registro o base de datos]	[Nombre del registro o base de datos]

Por parte de la ENTIDAD 1

La Entidad 1 se compromete a compartir las variables relacionadas en el diccionario de datos definido en este anexo.

Base de Datos 1: [Descripción de la base de datos o registro administrativo a compartir y de donde se obtienen los datos]. A la fecha se hace entrega mensual desde el año [XX]. No obstante, se cuenta con el diccionario acordado con la ENTIDAD 2 que, para efectos del presente Anexo Técnico, sería el siguiente:

Nro.	Nombre Variable	Campo Base Datos	Tipo de dato	Descripción de la variable	Valores válidos para la variable (dominio)	Clasificación de la variable (pública, clasificada o reservada)

Por parte de la ENTIDAD 2

Base de datos 1: [Descripción de la base de datos o registro administrativo a compartir y de donde se obtienen los datos]. A la fecha se hace entrega mensual desde el año [XX]. No obstante, se cuenta con el diccionario acordado con la ENTIDAD 1 que, para efectos del presente Anexo Técnico, sería el siguiente:

Nro.	Nombre Variable	Campo Base Datos	Tipo de dato	Descripción de la variable	Valores válidos para la variable (dominio)	Clasificación de la variable (pública, clasificada o reservada)

2. ESQUEMA DE INTERCAMBIO Y FORMA DE ACCESO

[Descripción del esquema que acuerden LAS PARTES]

3. PERIODICIDAD DEL INTERCAMBIO

[Descripción de la periodicidad que acuerden LAS PARTES]

4. MODIFICACIONES AL ANEXO TÉCNICO

El diccionario de datos y el esquema de intercambio y forma de acceso que hacen parte integral del presente anexo técnico podrán ser modificados cada vez que se realice una actualización al mismo, sin necesidad de modificar el anexo técnico. Bastará informar a cada una de LAS PARTES y la aprobación para la respectiva actualización, siempre y cuando se mantengan los términos del Acuerdo de transferencia o Intercambio de Información suscrito entre ambas partes.

5. DIRECTORIO DE CONTACTOS

Nombres	Entidad	Cargo	Correo	Teléfono
---------	---------	-------	--------	----------

--	--	--	--	--

El presente documento se firma a los XX días del mes de XX del año XX

LAS PARTES,

POR LA ENTIDAD 1
Nombre y cargo

POR LA ENTIDAD 2
Nombre y cargo

ANEXO 3

PERFIL DEL ADMINISTRADOR DE DATOS

1. Perfil

El Administrador de Datos es un líder estratégico y técnico que se encarga de la gestión integral de los datos y los procesos de intercambio e interoperabilidad de una entidad pública.

Este rol combina conocimiento técnico en materia de gestión y procesamiento de datos e implica un alto conocimiento procesos institucionales y los datos de negocio. Debe definir y ejecutar la estrategia de datos institucional para asegurar su valor, calidad, seguridad, interoperabilidad, gobernanza, uso y cumplimiento normativo.

En las entidades distritales, este rol es fundamental para impulsar la transformación digital y el Gobierno Digital, garantizando que la información sea un activo estratégico para la toma de decisiones y la prestación de trámites y servicios.

Este perfil debe hacer parte de los manuales de funciones de las entidades distritales, ideal que sea de planta, sin embargo, puede ser un contratista y la entidad debe asegurar la transferencia de conocimiento con el profesional de planta que tenga funciones relacionadas con la gestión de los datos.

El rol puede estar asociado a las oficinas de planeación, las direcciones u oficinas de tecnología o quien haga sus veces o a las oficinas o direcciones de gestión de información.

2. Competencias

1. Habilidad y conocimiento para gestionar proyectos.
2. Habilidad para coordinar y gestionar un equipo multidisciplinario.
3. Habilidad para colaborar y comunicarse de manera efectiva y asertiva con la alta dirección, las áreas funcionales organizaciones funcionales e individuos para priorizar y ejecutar proyectos de datos e interoperabilidad.
4. Capacidad para proporcionar información y orientación sobre gobernanza e interoperabilidad de datos.
5. Experiencia en la gestión y los procesos de datos durante todo su ciclo de vida.
6. Comprensión de todos los datos y procesos de la entidad, según el sector.
7. Capacidad para estructurar presentaciones y presentarlas eficazmente a la dirección.

3. Funciones específicas en materia de interoperabilidad

1. Coordinar y gestionar el proceso de intercambio de datos e interoperabilidad de acuerdo con el Marco de Interoperabilidad, los lineamientos establecidos por la Oficina Consejería Distrital de TIC y el Ministerio de TIC, así como los demás marcos normativos vigentes.

2. Analizar y proponer mejoras a los procesos institucionales relacionados con el intercambio de información.
3. Identificar oportunidades para mejorar u optimizar los procesos de interoperabilidad de la entidad.
4. Apoyar la estructuración y ejecución de los Acuerdos de Intercambio establecidos por las entidades Distritales.
5. Realizar seguimiento y reportar los indicadores de avance en materia de interoperabilidad de acuerdo con los planes o la estrategia de interoperabilidad establecidas a nivel institucional y distrital.
6. Gestionar la actualización del catálogo de servicios de intercambio de información, así como los datos maestros y de referencia de la entidad, en la herramienta y los formatos establecidos para tal fin.
7. Las establecidas en el artículo 2.2.24.3.9 del Decreto 1078 de 2015 y el artículo 18 del Decreto Distrital 575 de 2023.

ANEXO 4

ESQUEMA DE GOBERNANZA DE INTEROPERABILIDAD COMO PARTE DEL MODELO DE GOBERNANZA DE INFRAESTRUCTURA DE DATOS DEL DISTRITO

Propósito y articulación con el Decreto Distrital 575 de 2023

El presente esquema de gobernanza no constituye un modelo nuevo o independiente, sino que desarrolla y operacionaliza el componente de interoperabilidad previsto dentro del Modelo de Gobernanza de la Infraestructura de Datos del Distrito, establecido en el Decreto Distrital 575 de 2023, particularmente en su artículo 7, el cual define las instancias, roles y responsabilidades para la gestión, uso y aprovechamiento de los datos en el Distrito Capital.

Este anexo tiene como propósito orientar a las entidades distritales en la organización de sus procesos, roles y responsabilidades internas para la implementación del componente de interoperabilidad, asegurando la coherencia con las directrices estratégicas definidas a nivel distrital.

En términos operativos, este documento detalla la manera en que el modelo general de gobernanza establecido en el Decreto 575 de 2023 se aplica en la gestión cotidiana de la interoperabilidad al interior de cada entidad.

La articulación entre el nivel distrital y la aplicación institucional se presenta en la siguiente tabla:

Nivel de Gobernanza	Instancia o Rol a Nivel Distrital (Decreto 575 de 2023)	Instancia o Rol Correspondiente al Interior de la Entidad
Estratégico	Comité Distrital de Datos y Coordinador Distrital de Datos: Definen la visión, políticas, hojas de ruta y estándares de interoperabilidad para todo el Distrito.	Alta Dirección / Comité Institucional de Gestión y Desempeño: Define los objetivos institucionales en materia de interoperabilidad, asegurando su alineación con la misionalidad, el plan de acción institucional y los lineamientos distritales.
Táctico	Entidades de apoyo técnico: Brindan soporte, lineamientos y guías para la implementación.	Administrador de Datos: Traduce las decisiones estratégicas en un plan de trabajo interno, coordina la implementación de los lineamientos distritales y lidera la articulación entre las áreas misionales, tecnológicas y de datos de la entidad.
Operativo	Entidades ejecutoras de interoperabilidad: Implementan los servicios y casos de uso definidos.	Equipos técnicos y funcionales: Ejecutan las acciones de interoperabilidad (desarrollo de servicios, implementación de API, gestión de seguridad, pruebas y despliegue), bajo la coordinación del Administrador de Datos.

2. Ámbitos del esquema de gobernanza de interoperabilidad en la Entidad

Cada entidad distrital deberá adoptar y aplicar el presente esquema bajo el liderazgo del Administrador de Datos, quien será responsable de coordinar las acciones necesarias para garantizar

la correcta implementación de la interoperabilidad. Para tal fin, se definen los siguientes seis (6) ámbitos:



2.1. Instancias de decisión

a) La gobernanza de interoperabilidad se desarrolla en dos planos interrelacionados:

- i. **A nivel distrital**, bajo la dirección del Comité Distrital de Datos, que define las políticas, estándares y estrategias generales para todo el ecosistema.
- ii. **A nivel institucional**, dentro de cada entidad distrital, donde dichas directrices se adaptan a la planeación estratégica, misional y operativa de la entidad.

b) En el plano institucional, el proceso de decisión fluye desde el nivel estratégico hacia el nivel operativo, asegurando coherencia entre las metas de la entidad, su plan de acción institucional y los lineamientos distritales.

c) Cada entidad debe identificar dentro de su estructura las instancias o roles que representen los tres niveles de decisión descritos a continuación:

i. **Nivel estratégico interno:** Corresponde a la alta dirección o al Comité Institucional de Gestión y Desempeño, o quien haga sus veces, que orienta las decisiones estratégicas de la entidad. Este nivel debe garantizar que las acciones de interoperabilidad se encuentren alineadas con los objetivos misionales, el plan de acción y la planeación estratégica institucional.

ii. **Nivel táctico interno:** Liderado por el Administrador de Datos, quien traduce las decisiones estratégicas en un plan de trabajo interno, gestiona los recursos y coordina a las dependencias involucradas en la interoperabilidad.

iii. **Nivel operativo interno:** Conformado por los equipos técnicos y funcionales encargados de ejecutar las acciones definidas en el plan de trabajo (desarrolladores, arquitectos, responsables de seguridad, líderes funcionales, entre otros).

d) Esta estructura busca asegurar que las decisiones de interoperabilidad dentro de la entidad sean consistentes con las prioridades institucionales y, al mismo tiempo, contribuyan al cumplimiento de los lineamientos distritales definidos por el Comité Distrital de Datos.

2.2. Roles y responsabilidades internas

a) El Administrador de Datos coordinará un equipo multidisciplinario responsable de la ejecución del proceso de interoperabilidad.

b) Los roles mínimos requeridos son los siguientes:

Nivel	Rol	Responsabilidad dentro de la entidad
Estratégico	Alta Dirección o Comité Institucional (de Planeación, Dirección o Transformación Digital)	1. Definir la visión y objetivos institucionales en materia de interoperabilidad, asegurando su alineación con la planeación estratégica y las metas misionales de la entidad. 2. Aprobar las políticas, lineamientos y prioridades internas que orienten el desarrollo de los servicios de interoperabilidad. 3. Hacer seguimiento al cumplimiento de los objetivos institucionales en interoperabilidad y su contribución a las metas distritales.
Táctico	Administrador de Datos	1. Articular y coordinar el ejercicio de interoperabilidad al interior de la entidad, en coherencia con los lineamientos distritales. 2. Traducir las decisiones estratégicas en planes de acción internos y coordinar su implementación con los equipos técnicos y funcionales. 3. Hacer seguimiento a la hoja de ruta de interoperabilidad institucional y reportar avances y dificultades a la alta dirección. 4. Facilitar la aplicación de las políticas, estándares y lineamientos definidos a nivel distrital y estratégico interno.
Operativo	Oficial de Seguridad y de Protección de Datos (CISO/DPO)	1. Garantizar el cumplimiento de los lineamientos y controles de seguridad de la información y protección de datos personales en todas las etapas del ciclo de vida de la interoperabilidad. 2. Establecer, monitorear y validar los mecanismos técnicos y organizacionales que aseguren la integridad, confidencialidad y disponibilidad de los datos intercambiados. 3. Coordinar las acciones de gestión de riesgos asociados a la interoperabilidad y a los incidentes de seguridad.
	Líder o Experto en Datos	1. Asegurar la calidad, trazabilidad y consistencia de los datos utilizados en los procesos de interoperabilidad. 2. Definir criterios de estandarización y apoyar la creación de catálogos, diccionarios o modelos de datos interoperables.

		3. Verificar que los conjuntos de datos compartidos cumplan con los requisitos técnicos y semánticos definidos en los lineamientos distritales.
	Líder o Arquitecto de Infraestructura	1. Brindar soporte técnico y garantizar la integridad, disponibilidad y seguridad de la infraestructura tecnológica que soporta la interoperabilidad. 2. Supervisar la operación de los servicios interoperables, identificando riesgos técnicos y proponiendo acciones correctivas o preventivas.
	Desarrollador	1. Implementar los servicios y APIs necesarios para garantizar el intercambio efectivo de información. 2. Mantener y documentar los componentes técnicos de interoperabilidad, asegurando el cumplimiento de estándares y lineamientos institucionales y distritales. 3. Proponer ajustes técnicos o de diseño que mejoren la eficiencia y seguridad de los servicios.
	Líderes Funcionales o de Negocio	1. Identificar las necesidades de interoperabilidad derivadas de los procesos misionales y definir los requerimientos funcionales para el desarrollo de trámites, servicios o APIs. 2. Validar que los desarrollos técnicos respondan a los objetivos de negocio y aporten valor a la gestión institucional.

c) La asignación de roles y responsabilidades en materia de interoperabilidad deberá corresponder a las capacidades institucionales de cada entidad y a su nivel de madurez en la implementación de la infraestructura de datos. En aquellos casos donde no existan equipos especializados o roles diferenciados, las funciones descritas podrán ser asumidas por las personas o dependencias que actualmente gestionen los temas, siempre que se garantice el cumplimiento de las responsabilidades establecidas en este esquema.

2.3. Cooperación y colaboración

a) El Administrador de Datos actuará como punto de contacto oficial entre la entidad y las demás entidades distritales en materia de interoperabilidad.

b) Sus responsabilidades incluirán:

- i. Liderar la estructuración y negociación de los Acuerdos de Intercambio de Información.
- ii. Coordinar la participación de la entidad en mesas técnicas y funcionales interinstitucionales.
- iii. Promover la colaboración y el intercambio de buenas prácticas entre entidades.

2.4. Comunicaciones

a) La comunicación dentro del esquema de gobernanza de interoperabilidad será permanente, bidireccional y trazable.

b) El Administrador de Datos deberá:

- i. **Comunicar hacia adentro:** Difundir políticas, estándares y decisiones del Comité Distrital de Datos entre los equipos institucionales.
- ii. **Comunicar hacia afuera:** Reportar avances, dificultades y resultados al Coordinador Distrital de Datos, garantizando la visibilidad del progreso institucional y su alineación con el nivel distrital.

2.5. Monitoreo y control

- a) Cada entidad deberá establecer mecanismos de seguimiento y evaluación para medir la eficacia de su gestión en interoperabilidad.
- b) El Administrador de Datos será responsable de:
 - i. Definir y monitorear indicadores de desempeño (por ejemplo, número de acuerdos suscritos, tiempos de respuesta, disponibilidad de servicios).
 - ii. Implementar los mecanismos de reporte definidos por el Comité Distrital de Datos.
 - iii. Retroalimentar los resultados al nivel distrital, con el fin de fortalecer la mejora continua del ecosistema de interoperabilidad.

2.6. Políticas y lineamientos

- a) Las entidades deberán adoptar, aplicar y vigilar el cumplimiento de las políticas, lineamientos y estándares de interoperabilidad expedidos por el Comité Distrital de Datos.
- b) El Administrador de Datos garantizará que todos los proyectos, servicios y desarrollos de intercambio de información se ajusten a dichas directrices.
- c) El cumplimiento de estos lineamientos contribuirá a consolidar un ecosistema distrital de datos interoperable, coherente, seguro y sostenible.

ANEXO 5

LINEAMIENTOS Y ESPECIFICACIONES TÉCNICAS PARA EL DISEÑO DE API's Y SERVICIOS WEB DISTRITALES

La siguiente especificación de diseño es obligatoria en el diseño de API's y servicios web distritales para el intercambio de información y/o publicación en el repositorio de API's del Distrito.

Las siguientes especificaciones y lineamientos técnicos deben ser parte de las arquitecturas de referencia de sistemas de información y datos de las entidades distritales.

1. ¿QUÉ ES UN API?

Es el acrónimo en inglés de Application Program Interface. Un API es:

- Un servicio web
- Una interface basada en estándares que permite a las aplicaciones exponer su funcionalidad a otros sistemas de información o aplicaciones.
- Define cómo interactúa una aplicación con otra, de forma estructurada para facilitar la integración y el intercambio de información. Los desarrolladores de software crean un API para compartir la funcionalidad o los datos de una aplicación que han desarrollado, con cualquiera que desee aprovecharla.
- Los datos e información que ofrece un API pueden ser presentados a los usuarios finales en un contexto o proceso específico, por ejemplo, a través de una aplicación móvil, aplicación web o tablero de control.

Las API's se pueden categorizar como se muestra en la siguiente tabla:

Tabla 1. Categorización de las API's

Categoría	Definición
API Interna	Un API que es usada solamente dentro de una entidad para uso e intercambio entre aplicaciones o sistemas internos.
API externa	Un API que es provista por una entidad y consumida por una entidad externa a ella.
API pública o abierta.	Un API que es provista para el público en general y puede ser usada cualquier organización que la requiera. Las API's pueden tener requerimientos de control de acceso o tener acceso abierto y libre para cualquiera que lo requiera.

Fuente: CINTEL, 2025

2. PRINCIPIOS PARA EL DISEÑO DE API'S

El diseño de las API's distritales se debe regir por los siguientes principios:

Usabilidad: Asegura una buena experiencia de usuario para sus consumidores

Interoperabilidad: Habilita el intercambio de datos entre sistemas sin dependencias tecnológicas.

Reúso: Aprovecha los estándares y taxonomías existentes para evitar la duplicación de esfuerzos y facilita la reutilización de los servicios.

Estabilidad: Asegura la coherencia y la transparencia de los cambios mediante la comunicación y la gobernanza.

Extensibilidad: Ofrece flexibilidad para extender las API a nuevas partes interesadas y canales de negocio.

Bajo acoplamiento: Proporciona flexibilidad y ofrece baja dependencia de otros servicios para minimizar el impacto de los cambios en las operaciones de otras API's.

Granularidad: Proporciona el nivel adecuado de funcionalidad sin ser demasiado monolítico ni demasiado específico.

Privacidad: Debe establecer los controles adecuados para garantizar que se cumpla con la política y la normativa de privacidad de la entidad y del país.

3. LINEAMIENTOS Y ESTÁNDARES TÉCNICOS

3.1 PROTOCOLOS Y ESTILOS RECOMENDADOS

Todos los servicios web y API's que se consuman y expongan seguirán el estándar API REST y GraphQL como primera opción según se requiera y para sistemas legados que lo requieran se utilizará SOAP.

Tabla 2. Estándar API's

Criterio	REST	GraphQL
Modelo o enfoque	Basado en recursos y verbos HTTP (GET, POST, PUT, DELETE). Múltiples endpoints para diferentes recursos.	Lenguaje de consulta para APIs. Un único endpoint para todas las operaciones.
Casos de uso recomendados	APIs públicas/Abiertas: Para exponer conjuntos de datos (datasets) estáticos o con cambios predecibles y donde la simplicidad de consumo es clave. - CRUD¹ de Recursos Simples: Gestionar entidades bien definidas (ej., usuarios, documentos, trámites simples). - API's para transferencias masivas en batch: (Ej. Carga/descarga de archivos completos como se discutió anteriormente).	- Aplicaciones con Requisitos de Datos Variables: Especialmente útil para frontends (web, móvil) que necesitan datos flexibles y personalizados, reduciendo el número de llamadas a la API. - Agregación de Datos Complejos: Cuando se necesita combinar información de múltiples fuentes (microservicios, bases de datos diversas) en una sola respuesta. - Interfaces de Usuario Dinámicas: Donde la interfaz de usuario se adapta a diferentes

¹ CRUD es un acrónimo que significa Crear, Leer, Actualizar y Eliminar. En términos de bases de datos y aplicaciones, estas son las cuatro operaciones básicas que se pueden realizar sobre los datos.

Criterio	REST	GraphQL
		roles y muestra diferentes combinaciones de datos.
Web caché	Bueno. Utiliza los mecanismos de caché HTTP estándar (códigos de estado, encabezados como Cache-Control, ETag, Last-Modified). Esto permite a los navegadores almacenar en caché las respuestas de las solicitudes GET, reduciendo la carga del servidor y mejorando el tiempo de respuesta para peticiones repetidas.	Más complejo. Dado que casi todas las peticiones son POST al mismo endpoint con cuerpos de solicitud únicos, los mecanismos de caché HTTP estándar no son efectivos de forma nativa. Requiere implementar estrategias de caché a nivel de aplicación o en una capa de proxy que procese GraphQL.
Desempeño	El rendimiento depende en gran medida del diseño de los endpoints y de la optimización del lado del servidor. Puede ser ineficiente porque puede haber sobrecaptura o subcaptura (Over/under -fetching) - Over-fetching: Recibe más datos de los necesarios, desperdiciando ancho de banda. - Under-fetching: Necesita múltiples solicitudes para obtener todos los datos relacionados, aumentando la latencia de red.	Optimiza el ancho de banda: Solo los datos solicitados son transferidos. - Reduce la latencia: Una única solicitud de red puede obtener datos de múltiples recursos relacionados. - El rendimiento puede degradarse con consultas excesivamente complejas. Generalmente es más eficiente porque no sobrecaptura o subcaptura (Sin Over/Under-fetching).
Nivel de madurez	Bajo. Es más simple de entender, implementar y consumir. Los navegadores pueden explorar fácilmente los endpoints. La curva de aprendizaje es menor.	Alto. La sintaxis de consulta y el concepto de un único endpoint pueden ser confusos. Requiere herramientas de cliente más sofisticadas.
Volumen de datos	Se puede diseñar un endpoint específico para subir/descargar un lote de recursos, o se pueden usar APIs asíncronas para archivos. Funciona bien para procesos ETL/ELT o transferencias de archivos grandes.	Aunque GraphQL permite consultas grandes, su fuerte es la granularidad, no necesariamente la transferencia masiva de archivos binarios o data dumps. Podría combinarse con APIs REST para la fase de descarga de archivos.

3.2 MANEJO DE ERRORES

- Los proveedores de los servicios web o API's deben gestionar todas las excepciones relacionadas con el API y enviar los códigos de respuesta y las descripciones correspondientes en la respuesta. Los códigos de error y las descripciones deben compartirse con los consumidores del servicio o API en la documentación.
- Se debe gestionar tres tipos de errores:

Fallas en validación de reglas de negocio: validación de fechas, dominios de datos asociados a reglas de negocio, entre otros.

Fallas en validación técnica: autenticación incorrecta, falla en conexión a base de datos, entre otros.

Fallas de infraestructura: fallas de conectividad, indisponibilidad de servidores, entre otros.

- Se debe hacer uso de los códigos de estado HTTP: Usar los códigos de estado estándar de HTTP (2xx, 4xx, 5xx) para indicar el resultado de la solicitud y enviar el mensaje en español.

200 OK: Éxito general.

201 Created: Recurso creado exitosamente.

204 No Content: Solicitud exitosa, sin contenido para devolver.

400 Bad Request: Petición mal formada (ej., JSON inválido).

401 Unauthorized: Autenticación fallida

403 Forbidden: Autenticado, pero no autorizado para el recurso.

404 Not Found: Recurso no encontrado.

405 Method Not Allowed: Método HTTP no permitido para el recurso.

409 Conflict: Conflicto con el estado actual del recurso (ej., intento de crear un recurso duplicado).

429 Too Many Requests: Límite de solicitudes excedido.

500 Internal Server Error: Error genérico del servidor.

503 Service Unavailable: Servicio temporalmente no disponible.

- Los proveedores de servicios o API's deben gestionar todas las excepciones que puedan ocurrir al invocar el servicio o API publicado.
- Para los escenarios de publicación-suscripción, se debe implementar un mecanismo de reintento en caso de que falle la entrega del mensaje al servicio suscriptor. El mecanismo de reintento debe considerar el tiempo. No se trata solo de volver a intentar, sino de cómo y cuándo hacerlo para no sobrecargar el sistema ni generar retrasos innecesarios. Existen varias estrategias de reintento que incorporan el tiempo, las más comunes son:
 - **Reintento con retardo fijo:** Se espera un tiempo constante (por ejemplo, 5 segundos) entre cada intento.
 - **Reintento con retardo exponencial:** El tiempo de espera aumenta exponencialmente después de cada intento fallido (por ejemplo, 2, 4, 8, 16 segundos). Esto ayuda a evitar la sobrecarga del servicio suscriptor si el problema es persistente y le da más tiempo para recuperarse. Es la estrategia más recomendada.
 - **Reintento con jitter (aleatoriedad):** Se añade un pequeño retardo aleatorio al tiempo de espera, ya sea fijo o exponencial. Esto es crucial en entornos donde múltiples suscriptores podrían estar intentando reintentar al mismo tiempo, lo que podría crear una "estampida de reintentos". El *jitter* distribuye estos reintentos en el tiempo.

El tiempo de reintegro es el tiempo que se acuerda para restablecer la comunicación o el intercambio de información entre las partes involucradas, dicho tiempo se recomienda sea

acordado entre las entidades involucradas en la interoperabilidad para lo cual se recomienda realizar una configuración que el publicador para que comunique a el suscriptor.

3.3 SOLICITUDES DE DATOS

Se recomienda configurar las API y servicios para que respondan a las solicitudes de datos en modo PULL (sending) o PUSH (pushing) según el caso o escenario. Esto garantiza que el usuario de la API solo reciba la información que necesita.

PULL (Sending): El cliente pide los datos. Es como un cliente que va al servidor a comprar un producto.

PUSH (Pushing): El servidor entrega los datos. Es como un proveedor que le lleva el producto a la casa de un suscriptor.

Se recomienda que una API responda a la solicitud de forma completa y específica. Por ejemplo, una API debería responder a la solicitud "¿Está este usuario casado?" con un valor booleano. La respuesta no debe devolver más detalles de los necesarios y debe depender de la aplicación cliente para interpretarla correctamente.

3.4 ESTÁNDARES SEMÁNTICOS

Se debe hacer uso de Lenguaje Común de Intercambio definido por el Ministerio TIC. Para los datos de tipo estadístico se debe hacer uso de los estándares definidos por el DANE para mejorar la estandarización y el intercambio de datos y metadatos estadísticos, fomentando la coherencia y la interoperabilidad entre los sistemas.

3.5 AUDITORIA

Todas las API's distritales que se desarrollen deben guardar traza de auditoría y logs. Niveles de registro de logs. permiten monitorear el comportamiento de las API's, diagnosticar problemas rápidamente, garantizar la seguridad y cumplir con requisitos de auditoría y trazabilidad. El objetivo es capturar suficiente información para ser útil, sin generar un volumen excesivo de datos que dificulte el análisis o consuma demasiados recursos.

Las API's y servicios deben registrar los siguientes niveles de información en los LOG según corresponda. Los distintos niveles de registro se detallan a continuación.

Tabla 3. Niveles de Registro en LOG para APIs y Servicios

Nivel de registro	Descripción	Nivel de implementación
TRACE	Indica de manera más detallada la información que genera el registro DEBUG la cual es útil para realizar una depuración profunda y seguimiento paso a paso de la ejecución del código.	Deseable
DEBUG	Indica eventos informativos detallados que son más útiles para depurar una aplicación	Deseable
ERROR	Indica eventos de error que han causado un fallo en una parte específica de la operación, pero la aplicación en sí sigue funcionando.	Obligatorio
FATAL	Indica un error severo que ha causado la terminación o el colapso inminente de la aplicación o del servicio.	Obligatorio
WARN	Indica situaciones potencialmente problemáticas o inesperadas que no impiden la ejecución actual, pero que podrían conducir a un problema en el futuro.	Obligatorio
INFO	Indica mensajes informativos que resaltan el progreso o comportamiento de la aplicación a nivel general	Obligatorio
OFF	El rango más alto posible y está diseñado para desactivar el inicio de sesión	Deseable

Cada entrada de log debe incluir los siguientes datos mínimos para facilitar la búsqueda y el análisis.

- **Timestamp (Marca de Tiempo):** En formato ISO 8601 con zona horaria UTC (ej., 2025-07-07T20:49:41.000Z). Crucial para la correlación de eventos.
- **Log Level:** (INFO, WARN, ERROR, etc.)
- **Trace ID/Correlation ID:** Un identificador único que se propaga a través de todas las llamadas de la API y los servicios internos. Permite rastrear una solicitud completa a través de múltiples componentes. Esencial para microservicios.
- **Message (Mensaje):** Una descripción legible y concisa del evento.
- **API Endpoint:** La URL del endpoint de la API que se está invocando (ej., /api/v1/tramites/id).
- **Client IP Address:** Dirección IP del cliente que realiza la solicitud.
- **Service Name:** Nombre del servicio o microservicio que genera el log.
- **Component/Module:** El componente interno o módulo donde se generó el log.
- **Error Code (si es ERROR/FATAL):** Un código de error interno estandarizado que se pueda mapear a la documentación.

El Log nunca debe registrar información personal sensible (PII - Personally Identifiable Information), credenciales (contraseñas, tokens completos), datos financieros o cualquier otra información clasificada en los logs, independientemente del nivel de registro.

Para el registro de logs se debe preferir el formato JSON para los logs. Este facilita el procesamiento, la búsqueda y el análisis automatizado por parte de herramientas de gestión de logs.

El proveedor de un API o servicio debe configurar sistemas de monitoreo para generar alertas automáticas basadas en los niveles de log.

Alertas Obligatorias:

- **ERROR y FATAL:** Notificación inmediata a los equipos de operación y desarrollo.
- **WARN:** Notificación para revisión periódica o si la frecuencia excede un umbral.

3.6 MONITOREO

El proveedor de la API o servicio debe definir métricas clave de rendimiento (latencia, tasa de errores, volumen de solicitudes) y herramientas de monitoreo para asegurar el cumplimiento de los ANS (Acuerdos de Nivel de Servicio) establecidos.

4 VERSIONAMIENTO DE API'S Y SERVICIOS WEB.

El versionamiento semántico es el estándar que deberán utilizar todas las API's y servicios que se desarrollen y publiquen en el marketplace de API's del distrito. El versionamiento de las API's tiene como beneficios:

- Facilitar el consumo de API's.
- Mejorará la gobernanza de las APIS's
- Facilita la evolución del ecosistema y el Marketplace de APIs.

El formato que se deberá utilizar está basado en tres números Mayor. Menor. Parche, y cada componente tiene un significado específico:

Número Mayor (x.0.0):

Se incrementa el dígito cuando se introducen cambios incompatibles con versiones anteriores de la API. Esto significa que los clientes que usaban la versión anterior deberán realizar cambios en su código para adaptarse a la nueva versión. Ejemplos de cambio del número mayor:

- Eliminación de un endpoint o un campo obligatorio.
- Cambio de nombre de un endpoint o un parámetro.
- Modificación drástica de la estructura de un recurso (ej., de un arreglo a un objeto, o cambio de tipos de datos fundamentales).
- Cambios en la autenticación o autorización que requieran modificaciones en el cliente.

Número Menor (0.x.0):

Se incrementa el dígito cuando se agregan nuevas funcionalidades a la API que son compatibles con versiones anteriores. Los clientes existentes no deberían necesitar adaptar su código. Ejemplos de incrementos del número menor:

- Adición de un nuevo endpoint.
- Adición de un nuevo campo opcional a un recurso existente.
- Adición de nuevos valores a un enum existente.
- Mejoras de rendimiento o seguridad que no alteren la interfaz.

Número de Parche (0.0.x):

Se incrementa el dígito cuando se corrigen errores en la API, sin introducir cambios que afecten la compatibilidad con versiones anteriores. Ejemplos de incrementos del número de parche

- Corrección de un error en el cálculo de un dato.
- Arreglo de un problema de seguridad menor sin cambio de interfaz.
- Mejoras en la documentación de un endpoint sin cambios en el comportamiento.

Para las API's, es crucial cómo se expone esta versión a los consumidores. La estrategia que debe aplicarse es incluir la versión en la documentación y en la URI (Uniform Resource Identifier). Este versionamiento ofrece:

- Claridad inmediata para el cliente sobre la versión que está utilizando.

- Permite que varias versiones de la API coexistan simultáneamente, lo cual es vital durante la fase de transición de los clientes a una nueva versión.
 - Fácil de implementar y de gestionar en buses o gateways de API's.
- Ejemplo:

Se tiene la siguiente API del Distrito para consultar información de movilidad:

Primera versión de la API de semáforos:

<https://api.bogota.gov.co/v1/movilidad/semaforos>

<https://api.bogota.gov.co/v1/movilidad/semaforos?estado=operativo>

- Se añade un nuevo parámetro estado para filtrar semáforos operativos. Esto es un cambio Menor y sigue siendo v1. La URL no cambia, solo la documentación lo debe reflejar.

<https://api.bogota.gov.co/v1/movilidad/parqueaderos>

- Se añade un nuevo endpoint para parqueaderos. Esto es un cambio Menor y sigue siendo v1.

<https://api.bogota.gov.co/v2/movilidad/semaforos>

- Se decide que la estructura de respuesta para los semáforos cambiará drásticamente (ej., en v1 se devolvía una lista plana, en v2 se agrupará por comuna). Esto es un cambio Mayor, por lo que se introduce v2.
- Durante un período de tiempo (ej., 6 meses), v1 y v2 coexisten. Los clientes de v1 siguen funcionando mientras migran a v2.
- Después del período de gracia, v1 se desactiva.

5 FORMATOS DE INTERCAMBIO DE DATOS Y CODIFICACIÓN.

Los formatos para el intercambio de Datos que se deben utilizar como primera opción son:

- **JSON (JavaScript Object Notation).**
- **CVS.** Cuando no sea posible por JSON
- **GeoJson** para intercambio de información geográfica

Para el intercambio de datos geográficos dependiendo del propósito y en los casos donde el formato GeoJson no cumple con todas las expectativas se puede utilizar SHP o GeoDatabase según el caso.

Se debe utilizar el estándar de formato de transformación Unicode (UTF-8) al codificar texto u otras representaciones textuales de datos.

6 SEGURIDAD DE LAS API'S

- Todos los servicios web y API's deben soportar IPv6 y utilizar el esquema de direccionamiento RFC 3986.
- Los proveedores de servicios deben garantizar la implementación de mecanismos de autenticación y autorización adecuados para las API's.

² Especificación estándar que define la sintaxis genérica de un Identificador Uniforme de Recursos (URI). Un URI es una cadena de caracteres compacta que identifica un recurso abstracto o físico. En el desarrollo de APIs, especialmente en APIs RESTful, los URIs son el mecanismo principal para referenciar recursos.

- Los consumidores de servicios o API's deben garantizar el uso adecuado de la información compartida por los proveedores de servicios.

6.1 AUTENTICACIÓN

Se puede utilizar alguna de las siguientes opciones de acuerdo con el nivel de madurez y seguridad requerida

- **OAuth 2.0 (Recomendado):** Estándar para autorización. Permite delegar la autorización de acceso a los recursos.
- **JSON Web Tokens (JWT):** Utilizado frecuentemente con OAuth 2.0 como token de acceso. Permite verificar la identidad y permisos de forma descentralizada.
- **API Keys (Para casos simples/legados o bajo control estricto):** Un token único enviado en el encabezado o como parámetro de consulta. Menos seguro que OAuth, pero más fácil de implementar para entidades con baja madurez.

Para invocar un API o servicio publicado, un consumidor de servicios necesita, como mínimo, autenticación básica HTTP sobre SSL. Se implementarán mecanismos de seguridad adicionales dentro del proveedor de servicios en función de la naturaleza confidencial del servicio.

6.2 AUTORIZACIÓN

Se puede utilizar alguna de las siguientes estrategias según el nivel requerido:

- **RBAC (Role-Based Access Control):** Basar los permisos en roles predefinidos.
- **ABAC (Attribute-Based Access Control):** Para escenarios más complejos, los permisos se basan en atributos del usuario, recurso y contexto.

6.3 SEGURIDAD CAPA DE TRANSPORTE

HTTPS (HTTP Secure): es de uso obligatorio y es la versión segura de HTTP, utilizando SSL/TLS para cifrar la comunicación. Garantiza la **confidencialidad** (los datos no pueden ser leídos por terceros), la **integridad** (los datos no han sido alterados en tránsito) y la **autenticación** (se verifica la identidad del servidor).

Versiones de TLS: se debe configurar TLS 1.2 o superior para la comunicación segura, deshabilitando versiones antiguas y vulnerables (TLS 1.0, 1.1 y SSLv3).

Las API's deben clasificarse de acuerdo con la categoría de los datos que ofrecen, de acuerdo con la siguiente tabla:

Tabla 3. Niveles clasificación API's

Categoría API	Clasificación
Alta	Reservado
Media	Clasificada
Baja	Publica

6.4 LIMITES O TASAS

Para proteger la API de abusos y garantizar la disponibilidad se debe establecer el límite de solicitudes simultaneas o concurrentes en un tiempo específicos, límites de tiempos de respuesta y explicar qué sucederá si los usuarios superan ese límite, incluyendo el tipo de mensaje de error que pueden esperar.

6.5 VALIDACIÓN DE ENTRADA

Validar todos los datos recibidos para prevenir inyecciones (SQL Injection, XSS) y otros ataques.

7 DOCUMENTACIÓN DEL API

Todas las API's o servicios web que se desarrollen para el intercambio de datos e interoperabilidad de datos estructurados y que se publiquen en el repositorio de API's del Distrito deben seguir la especificación OpenAPI Specification (OAS), el cual es un estándar abierto e independiente de proveedores para describir API's RESTful. El aplicar esta especificación permite que las API's sean claras, bien documentadas, fáciles de consumir y que su desarrollo sea más eficiente y menos propenso a errores.

Para las API's o servicios web que manejan e intercambian datos geográficos se debe usar la especificación OGC API desarrollada por Open Geospatial Consortium (OGC), la cual es la organización líder en el desarrollo de estándares para datos geográficos.

Beneficios de utilizar **OpenAPI Specification**.

- **Permite generar documentación automática e interactiva:** a través de herramientas como Swagger se puede tomar un archivo OpenAPI y generar automáticamente un portal de documentación interactivo y fácil de usar, donde los desarrolladores pueden ver los endpoints, sus parámetros y hasta probar las API's directamente en el navegador.
- **Permite automatización de pruebas:** Las herramientas de prueba pueden leer el archivo OpenAPI para generar automáticamente casos de prueba, verificar la conformidad de las respuestas y monitorear la salud de la API.

De acuerdo con la Especificación OPEN API, el contrato de servicio de la API o servicio web debe tener como mínimo la siguiente información, el cual será publicado y requerido para la publicación en el repositorio o Marketplace de API's del Distrito:

Información de la API

1. **Título, versión y descripción:** Proporciona información general sobre la API, incluyendo su nombre, la versión actual (siguiendo el versionado semántico: MAYOR.MENOR. PARCHE).
2. **Método de autenticación:** Describe cómo los usuarios o sistemas deben autenticarse para acceder a la API (por ejemplo, claves API, OAuth2, autenticación básica).
3. **Ubicación de los servidores de la API:** Indica las URLs base donde se aloja la API.

Puntos finales (Paths y Endpoints)

4. Define las diversas rutas (paths) de la API, que son las URLs específicas que un cliente puede usar para interactuar con ella (por ejemplo, /users).

5. Para cada ruta, se especifican los métodos HTTP que soporta (como GET, POST, PUT, DELETE) y lo que la API debe hacer cuando se realiza una solicitud a esa ruta.
6. Cada operación debe incluir:
 - **Resumen y descripción:** Una breve explicación y una información más detallada sobre la funcionalidad de la operación.
 - **Parámetros:** Las entradas necesarias para la llamada a la API, como parámetros de consulta (query), de ruta (path) o de cabecera (header).
 - **Formatos de respuesta:** Para cada posible código de respuesta HTTP (incluyendo errores), se documenta el código de estado, las cabeceras de respuesta y el formato del cuerpo de la respuesta. Es obligatorio proporcionar retroalimentación específica en las respuestas de error, de acuerdo con lo indicado en el numeral de esta guía.

Modelos de solicitud y respuesta

Permiten definir elementos que pueden ser utilizados en múltiples puntos finales (end points) de la API, como parámetros comunes, formatos de solicitud y respuesta, y esquemas de datos.

- Los **Modelos de Solicitud (Request Models)** definen la estructura de los datos que un cliente envía a la API, incluyendo el formato esperado (JSON o XML) y los campos requeridos.
- Los **Modelos de Respuesta (Response Models)** describen lo que la API devuelve después de procesar una solicitud, incluyendo el código de estado y un esquema que describe la estructura de los datos devueltos.

8 ACUERDOS DE NIVEL DE SERVICIO

Todos los servicios que se publiquen a plataforma o catálogo de API's del Distrito y se desarrollen para interoperar deben establecer los ANS especificados en el siguiente formato:

ACUERDO DE NIVEL DE SERVICIO ENTRE LA ENTIDAD XXX Y LA ENTIDAD PROVEEDORA DEL API O SERVICIO WEB

CONTROL DE VERSIONES

Versión (1)	Fecha (2)	Descripción (3)	Autor ⁽⁴⁾	
			Nombres y Apellidos	Cargo
1.0.0				
...				
"n"				
Consideraciones Para el control de versiones considerar lo siguiente: (1) Versión³: Las versiones se expresan con números, el formato que se debe utilizar para versionar es el versionamiento semántico. • Versión Mayor = "1.0.0" Incrementar el primer decimal generalmente indica una actualización o cambio sustancial en el servicio.				

³ Se ha tomado como referencia el versionado semántico (o en inglés Semantic Versioning).

Cuando hay un cambio en esta versión las demás deben volver a “0”. Más decimales conducen a versiones más detalladas.

Cambio sustancial en la versión: 1.0.0 à 2.0.0 à 3.0.0

- **Versión Menor = "1.1.0"**

Los decimales después del primer número suelen representar varios cambios menores de la versión.

Cambios menores en la versión: 1.0.0 à 1.1.0 à 1.2.0

- **Versión parche = "1.1.1"**

Considerar incrementos en esta versión cuando se introducen solo arreglos compatibles con la versión anterior. Puede considerarse algún cambio que no modifica las condiciones del servicio.

Cambios internos en la versión: 1.0.0 à 1.0.1 à 1.0.2

- (2) **Fecha:** Indicar el día, mes y año que se actualizó la versión del ANS. El formato es DD/MM/AAAA.
- (3) **Descripción:** Elaborar un breve resumen de los cambios realizados respecto a la versión anterior, cuando corresponda.
- (4) **Autor:** Indicar el nombre(s) y cargo(s) de la persona que ha(n) desarrollado la versión vigente del ANS.

El **ACUERDO DE NIVEL DE SERVICIO (ANS)** que celebran entre entidad XXXX en lo sucesivo **Entidad consumidora** y de la otra parte, “**NOMBRE DE LA ENTIDAD PROVEEDORA DEL API o servicio**”, en adelante **EL PROVEEDOR**, que las partes establecen en el marco de los lineamientos dispuestos por la Oficina Consejería Distrital de Tecnologías de la Información y las Comunicaciones en el anexo 3: Lineamientos y especificaciones técnicas para el diseño de API's distritales en los siguientes términos:

1. **Acuerdo General:** Este documento representa un compromiso entre EL PROVEEDOR y la entidad consumidora, para brindar el soporte técnico y la sostenibilidad operativa a la API(s) o servicio(s) dispuestos para el intercambio de datos o interoperabilidad.
Este ACUERDO DE NIVEL DE SERVICIO (en adelante “ANS”) será válido hasta que sea reemplazado por otra versión de este, debidamente revisada, aprobada y que garantice mejoras del servicio o API.
2. **Propósito y Objetivo:** El ANS se constituye en un instrumento de gestión formal entre las partes interesadas, el cual refleja los compromisos de EL PROVEEDOR y entidad consumidora para asegurar la disponibilidad, capacidad y escalabilidad de los servicios o API(s).

El ANS tiene como objetivos:

1. Establecer las responsabilidades y obligaciones vinculadas a los servicios publicados por parte de EL PROVEEDOR y entidad consumidora.

2. Asegurar los niveles de disponibilidad, capacidad y escalabilidad de los servicios o API(s) dispuestas.
 3. Indicar las restricciones para el uso de los servicios o API(s).
3. **Descripción del Servicio:** EL PROVEEDOR pone a disposición de entidad consumidora el (los) siguiente(s) servicio(s) o API(s):

Nº	Nombre del API o Servicio ⁽¹⁾	Descripción de la API o Servicio ⁽²⁾	Especificaciones del API o Servicio ⁽³⁾	Restricciones del API o Servicio ⁽⁴⁾
1				
...				
"n"				

Aspectos:

- (1) **Nombre del API o Servicio:** Indicar el nombre del(os) Web Service(s) o API(s) proporcionado(s) por EL PROVEEDOR a La entidad consumidora.
- (2) **Descripción del API o Servicio:** Indicar una breve descripción de los datos e información que proporciona el(os) Web Service(s) o API(s).
- (3) **Especificaciones:** Descripción de las características técnicas del(os) Web Service(s) a brindar (protocolos, estándares, lenguajes, etc.); así como los parámetros de entrada y salida. Se debe referenciar al enlace del repositorio de API(s) del distrito donde queda dispuesto el API para descarga y consulta de la documentación o el documento que soporta la documentación técnica.
- (4) **Restricciones del API o Servicio:** Indica las restricciones legales, técnicas o de seguridad para el uso o acceso a los servicios o API(s). Ejemplos: transacciones por segundo, transacciones por usuario, transacciones por entidad y horarios de funcionamiento del servicio.

4. **Gestión del Servicio:** Con la finalidad de asegurar la disponibilidad, capacidad y escalabilidad del servicio, EL PROVEEDOR especifica dichos parámetros en el formato siguiente:

Nombre de API o Servicio ⁽¹⁾	Horas Acordadas				Disponibilidad ⁽⁶⁾	Tiempo de Respuesta ⁽⁷⁾		Número máximo de solicitudes concurrentes ⁽⁸⁾	
	Horas ⁽²⁾	Días ⁽³⁾	HS A ⁽⁴⁾	HS S ⁽⁵⁾					

Aspectos:

- (1) **Nombre del API o Servicio:** Indicar el nombre del(os) API(s) o Web Service(s) proporcionado(s) por EL PROVEEDOR a entidad consumidora.
- (2) **Horas:** Indicar el número de horas al día de disponibilidad del(os) API(s) o Web Service(s).
- (3) **Días:** Indicar el número de días al mes de disponibilidad del(os) API(s) o Web Service(s). Se debe considerar 30 días como valor referencial.
- (4) **HSA - Horas de Servicio Acordado:** Indica el número de horas que el(os) API(s) o Web Service(s) está(n) disponible(s) al mes. Se obtiene mediante la multiplicación de (2) por (3).

- (5) **HIS - Horas de Inactividad del Servicio:** Indicar el número de horas que el(os) API(s) o Web Service(s) se encuentra(n) inoperativo(s).
- (6) **Disponibilidad:** Indica el porcentaje del tiempo mensual que EL PROVEEDOR se compromete a que el(ds) servicio(s) estará(n) disponible(s) para su uso⁴. La disponibilidad se expresa en porcentaje y es medida con la siguiente fórmula:

$$\text{Disponibilidad} = \left(\frac{HSA - HIS}{HSA} \right) * 100$$

**** No se considera Horas de Inactividad del Servicio - HIS:**

- Cortes de energía atribuibles a terceros que afectan las telecomunicaciones, servidores, computadoras que dan respaldo al servicio.
 - Caída de enlaces de comunicaciones que no estén bajo la administración de EL PROVEEDOR.
 - Fallas en las aplicaciones de software que afecten el servicio y que no estén bajo la administración de EL PROVEEDOR.
 - Averías o daños parciales o totales causados por usos incorrectos de los usuarios.
 - Ciberataques que ocasionen la imposibilidad total o parcial en la prestación del servicio.
 - Averías externas no imputables a EL PROVEEDOR.
- (7) **Tiempo de respuesta.** Indicar la rapidez con la que las API(s) o servicio(s) deben responder en milisegundos.
- (8) **Número máximo de solicitudes concurrentes:** Indicar la cantidad de solicitudes o transacciones concurrentes que pueden ser soportadas por el servicio en un determinado periodo (usualmente medido en transacciones por segundo TPS).

5. Atención de requerimientos e incidentes: Con la finalidad de contar con una adecuada gestión de los requerimientos, incidentes o errores relacionados con la API(s) o servicio(s), EL PROVEEDOR y La entidad consumidora dispone de los siguientes canales y niveles de atención.

Mesa de servicio				
Canal		Detalle ⁽¹⁾		Horario ⁽²⁾
Soporte telefónico:				
Soporte por correo electrónico:				
Niveles de Atención de requerimientos, incidentes o errores ⁽³⁾				
Nivel	Nombre	Cargo	Teléfono	Correo
1				
2				
3				
Nomenclatura:				

⁴ La disponibilidad de un servicio es la capacidad de completar satisfactoriamente una transacción de negocio, en ese sentido, los cálculos para determinar la disponibilidad de un servicio deben considerar las horas estándar de sus operaciones. La mayoría de las áreas de TI en las organizaciones tienen definidas actividades de mantenimiento (también conocida como “ventana de mantenimiento”) para sus aplicaciones, base de datos e infraestructura. Consecuentemente, los cálculos de la disponibilidad del servicio considerasen dichas interrupciones planificadas junto con su correspondiente horario. El horario estándar de operación variará dependiendo de la naturaleza y críticamente de cada servicio. La disponibilidad es el factor más importante que influye en la percepción de la calidad del servicio de TI en los usuarios. También es el factor más crítico que afecta a la productividad del usuario, especialmente si el usuario depende totalmente de una aplicación de negocio particular para realizar su función de trabajo. Tomado y adaptado de Foundations of Service Level Management (Rick Sturm, Wayne Morris y Mary Jander).

- (1) **Detalle:** Indicar el número telefónico, anexo o correo electrónico u otros que EL PROVEEDOR establezca como canal de atención de los requerimientos incidentes o errores presentados en el API o web service.
- (2) **Horario:** Indicar los días y horario de atención de la Mesa de servicio o Central telefónica para atender los requerimientos o incidencias del API o web service publicado (Por ejemplo: L-V de 8:00 A.M. a 8:00 P.M. / L-V de 9:00 A.M. a 9:00 P.M., etc.)
- (3) **Niveles de atención:** Se detalla el nombre, teléfono, cargo y e-mail del responsable de atender el requerimiento, incidente o error, según el nivel que corresponda. Se deben contemplar tres (03) niveles de atención, donde los niveles 1 y 3 son:
 - **Nivel 1:** Definido por la entidad
 - **Nivel 2:** Definido por la entidad
 - **Nivel 3:** Definido por la entidad

6. **Responsabilidades:** Las partes interesadas tendrán las siguientes responsabilidades:

a) EL PROVEEDOR

Nº	Responsabilidades de EL PROVEEDOR ⁽¹⁾
1	
...	
"n"	
(1) Responsabilidades de EL PROVEEDOR: Comprende los compromisos que son asumidos por EL PROVEEDOR para asegurar la disponibilidad, capacidad y escalabilidad del API o Servicios Web dispuestos. Puede considerar como referencia los siguientes: • Entregar y asegurar la disponibilidad del(os) API(s) o Servicios(s) web según se especifica(n) en el ANS. • Asegurar la disponibilidad del(os) Servicio(s) web, según lo especificado en el presente ANS. • Comunicar oportunamente a la entidad consumidora ante cualquier plan, programa o actividad de mantenimiento del(as) API(s) o Servicio web(s), mediante los mecanismos anteriormente indicados. • Comunicar y documentar los cambios o actualizaciones en los API(s) o Servicio(s) Web. • Registrar, atender y monitorear todas las incidencias reportadas por la entidad consumidora. • Cumplir los plazos de atención para los incidentes reportados por La entidad consumidora u otros, conforme a lo acordado en el ANS. • Gestionar la documentación apropiada para resolver las incidencias en el futuro. • Respetar los tiempos para escalar los requerimientos o incidentes, según lo especificado en el presente ANS. • Conocer el contenido del ANS.	

b) La entidad consumidora

N	Responsabilidades de entidad consumidora ⁽²⁾
1	
2..	
n	
(2) Responsabilidades de la entidad consumidora: Comprende los compromisos que son asumidos por la entidad consumidora. Puede considerar como referencia los siguientes: • Mantener la confidencialidad de la información sobre las API(s) o servicios que están publicados el repositorio de API(s) del Distrito o fueron suministradas. • Respetar los tiempos para escalar los requerimientos o averías, según lo especificado en el presente ANS. • Informar sobre cualquier incumplimiento del(os) servicio(s) o API(s).	

7. Suscripción del Acuerdo de Nivel de Servicio

El presente Acuerdo de Nivel de Servicio se suscribe de común acuerdo entre las partes interesadas, a fin de que se asegure la disponibilidad, capacidad y escalabilidad de las API(s) y servicio(s).

En concordancia con lo anterior y en señal de conformidad y aceptación, las partes suscriben el presente Acuerdo de Nivel de Servicio, en la ciudad de Bogotá D.C a los __ días del mes de _____ del año ____.

Firmas

Cargo del firmante
(Entidad consumidora)
(Nombre del Área)
(Nombre de la entidad)

Cargo del firmante
(EL PROVEEDOR)
(Nombre del Área)
(Nombre de la entidad)