

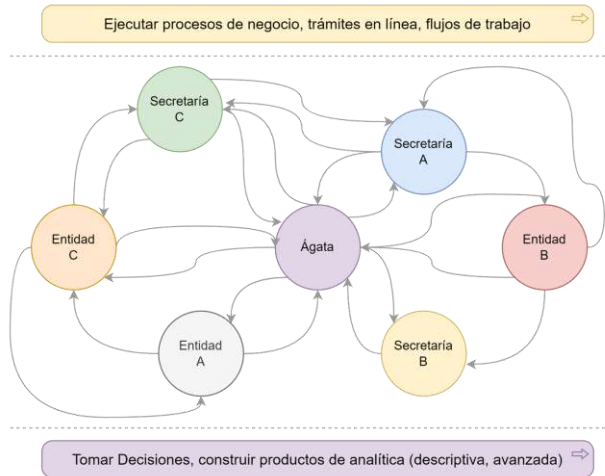
# INTEROPERABILIDAD SEGURA DE LOS DATOS PERSONALES

ÁGATA

29 de Agosto de 2023

# 0. Qué es interoperabilidad?

La interoperabilidad de datos es igual para los diferentes propósitos de uso de los datos (**transaccionales o analítica**)?



## DEFINICIONES:

- Es la capacidad que tiene un sistema para comunicarse (entrada/salida) o intercambiar datos con otros y los otros con él mismo.
- El intercambio de datos con una comunicación o interacción se entiende generalmente como bidireccional (en 2 vías, de entrada y salida)

**VISIÓN:** Sistemas de información bidireccionales para la colaboración, actualización, interoperabilidad y uso confiable de datos.

Junto con la continua evolución de los sistemas de gestión de datos para los nuevos requisitos del mercado, **estamos pasando de sistemas centralizados a sistemas descentralizados**, donde los datos se mantienen en diferentes sitios con capacidades autónomas de almacenamiento y computación.

Hay dos problemas fundamentales con estos sistemas descentralizados: privacidad local y consistencia global.

1. **Mediante la privacidad local**, el propietario de los datos desea controlar qué información debe exponerse y cómo otros pares deben usarla o actualizarla.
2. **Por consistencia global**, los sistemas desean tener una visión globalmente consistente e integrada de todos los datos.

# 1. Garantía de seguridad y privacidad de los datos

¿De qué forma se garantiza la seguridad y privacidad de los datos en la prestación de trámites y servicios en línea con los mecanismos de interoperabilidad?

- La aplicación racional del **principio de minimización de datos**, bajo los criterios de adecuación, pertinencia y necesidad con relación a los fines en el diseño de las distintas fases del tratamiento de los datos.
- Además, **la seguridad de la información debe estar siempre** por defecto en todos los sistemas, transferencias, soluciones y opciones cuando se tratan datos personales.
- Estas medidas incluyen la seudonimización y el cifrado de los datos personales, garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y los servicios de tratamiento, tener la capacidad de restaurar la disponibilidad y el acceso a los datos personales lo más rápidamente que sea posible, tras sufrir un incidente físico o técnico.
- Es importante tener en cuenta que estas medidas son solo algunas recomendaciones para garantizar la seguridad y privacidad en el manejo de datos personales. **Cada organización debe evaluar sus propias necesidades** y riesgos para determinar qué medidas son las más adecuadas para su situación específica.

## 2. Criterios de seguridad y privacidad

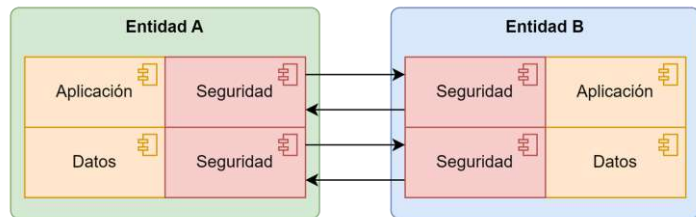
¿Cuáles son los criterios de seguridad y privacidad que se deben tener en cuenta en la interoperabilidad de datos personales?

En resumen, algunos criterios importantes a tener en cuenta para garantizar la seguridad y privacidad en la interoperabilidad de datos personales en Colombia son:

- Identificar claramente quiénes son los **responsables y encargados** del tratamiento de los datos.
- Garantizar en todo tiempo el pleno y efectivo ejercicio del **derecho de Hábeas Data**.
- Informar al momento de solicitar la autorización para el tratamiento de datos las **finalidades específicas** a las cuales serán sometidos esos datos.
- Mantener una copia de la respectiva **autorización otorgada por el titular** para el tratamiento de datos.
- Contar con canales necesarios al interior para **tramitar las consultas o reclamos** formulados en los términos de la ley.

### 3. Infraestructura de seguridad y privacidad

Cómo garantizan los operadores de interoperabilidad que su infraestructura cumpla con las garantías de seguridad y privacidad en el tratamiento de datos personales?



- Con la implementación de **medidas técnicas y organizacionales adecuadas**. Estas medidas incluyen, entre otras, la cifrado de datos, la autenticación de usuarios, la gestión de identidades y accesos, la realización de auditorías y evaluaciones de riesgos, y el cumplimiento de las normativas y regulaciones aplicables.
- Es importante destacar que los operadores de interoperabilidad deben **cumplir con los principios fundamentales del tratamiento de datos personales**, como la transparencia, la finalidad legítima, la minimización de datos, la exactitud, la limitación del plazo de conservación, la integridad y confidencialidad, y la responsabilidad proactiva.

## 4. Protección de los datos de los ciudadanos

En el proceso de intercambio de información, para los efectos interoperabilidad como se protegen los datos que pertenecen a los ciudadanos?

Los datos que pertenecen a los ciudadanos se protegen a través de la aplicación de los siguientes principios:

- **Principio de finalidad:** Los datos personales deben ser recogidos con fines determinados, explícitos y legítimos, y no podrán ser tratados posteriormente de manera incompatible con dichos fines.
- **Principio de calidad:** Los datos personales deben ser adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.
- **Principio de seguridad:** Los responsables del tratamiento deben adoptar las medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad y confidencialidad de los datos personales.

Además, existen medidas específicas que se pueden tomar para proteger los datos personales en el intercambio de información. Algunas de estas medidas son:

- **Cifrado de datos:** La información se puede cifrar para que solo pueda ser leída por las personas autorizadas.
- **Controles de autenticación y autorización:** Despliegue de mecanismos o recursos que permiten verificar la autenticidad e integridad del componente electrónico transmitido (transacción, datos, lotes de datos, streams).
- **Acceso restringido:** El acceso a la información se puede restringir a las personas autorizadas.

Es importante tener en cuenta que estas medidas no son exhaustivas y que cada caso debe ser evaluado individualmente para determinar las medidas adecuadas para proteger los datos personales

## 5. Estándares o normatividad aplicable

Qué estándares o normatividad aplicable se debe tener en cuenta para aplicar una interoperabilidad segura de datos personales?

- En Colombia, la **Ley 1581** de 2012 establece el régimen general de protección de datos personales, esta ley también regula el tratamiento de los datos sensibles.
- La **Ley 1712** de 2014 regula el derecho de acceso a la información pública.
- Para aplicar una interoperabilidad segura de datos personales en Colombia, se deben tener en cuenta los estándares y normatividad establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (**MINTIC**). El **Marco de Interoperabilidad para Gobierno Digital** es una estructura de trabajo común que alinea los conceptos y criterios que guían el intercambio de información entre los sistemas de los diferentes actores que prestan y/o demandan trámites y/o servicios del Estado Colombiano
- **La guía de calidad estándares de calidad e interoperabilidad de datos (MINTIC)** proporciona orientaciones y buenas prácticas para el desarrollo de estrategias de apertura de datos, que cumplen con los principales estándares de calidad e interoperabilidad de datos abiertos a nivel internacional, con base en el análisis de **17 criterios fundamentales de calidad de datos**, principios para la publicación y calidad de metadatos.
- La norma **ISO/IEC 27018:2019** es un código de prácticas diseñado para proteger datos personales en la nube. Se basa en la norma ISO/IEC de seguridad de la información 27002 y proporciona pautas de implementación sobre los controles IEC/IEC 27002 aplicables a la información personalmente identificable (PII) en la nube pública.

## 6. Clasificación de la información

Como se clasifica la información que es intercambiada mediante servicios en línea?

Los datos que se intercambian mediante servicios en línea en Colombia se pueden clasificar en diferentes categorías.

- Una de las categorías es la de **datos abiertos**. Los datos abiertos son aquellos que están disponibles para cualquier persona, sin restricciones de uso, distribución o acceso, y que se publican en formatos que permiten su reutilización.
- Otra categoría es la de **datos personales**. Estos datos son aquellos que identifican a una persona, como su nombre, dirección, número de identificación, entre otros. En Colombia,
- Además, existe la categoría de **datos sensibles**, que son aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación. Estos datos incluyen información sobre la salud, la orientación sexual, las creencias religiosas, entre otros.



## 7. Recomendación para la aplicación de controles

Cuáles son las recomendaciones a tener en cuenta en la aplicación de controles de seguridad y privacidad para la interoperabilidad segura de datos personales.

- Toda la información de los usuarios que se genere, almacene, transmita o trate en el marco de los **servicios ciudadanos digitales deberá ser protegida y custodiada bajo los más estrictos esquemas de seguridad digital y privacidad** con miras a garantizar la autenticidad, integridad, disponibilidad, confidencialidad, el acceso y circulación restringida de la información.
- Tener muy claro los requerimientos (funcionales y no funcionales) específicos del uso de los datos.
- Primero diseño, luego implemento, construyo o desarrollo.
- Asegurar los datos por cada flujo de ejecución o uso.
- Tener en cuenta la eficiencia operativa.
- Validación de costos.
- Reuso de componentes y recursos para la aplicación de controles de seguridad y privacidad.
- Cada organización debe evaluar sus propias necesidades y riesgos para determinar qué controles son los más adecuados para su situación específica.

GR4CIAS



ALCALDÍA MAJOR  
DE BOGOTÁ D.C.

SECRETARÍA DE  
SALUD

BOGOTÁ

# Bogotá Salud Digital

En agosto de 2019, se desplegó en la Red Pública la Plataforma tecnológica de Bogotá Salud Digital, un hito significativo que marcó un paso crucial hacia la interoperabilidad de la Historia Clínica Electrónica Unificada provista por las Subredes Integradas de Servicios de Salud. Esta implementación representó una colaboración estratégica que unió los esfuerzos de múltiples instituciones de salud para lograr un acceso más integral y coordinado a la información médica de los pacientes. Con esta plataforma en funcionamiento, los profesionales de la salud lograron acceder a los registros clínicos electrónicos de manera rápida y precisa



# ¿Qué es?

Es la Plataforma tecnológica de interoperabilidad en Salud del Distrito Capital, que dispone servicios ciudadanos digitales en salud a través del acceso, intercambio e integración de la información electrónica en salud entre los diferentes actores del sistema, que permite:



- Gestionar sus citas médicas (solicitar, hacer seguimiento, cancelar)
- Hacer seguimiento a sus ordenes de medicamentos (formulación, autorización, dispensación).
- Tener acceso a su Historia clínica sin necesidad de imprimir.



- Acceso en línea a la historia clínica, resultados de laboratorio e imágenes diagnosticas del paciente.
- Acceso al historial de medicamentos del paciente.



- Reducción de costos: mayor control de las prestaciones, menos pruebas duplicadas y menos papel.
- Impulsa la autonomía de cada institución y facilita la integración con otros operadores.



# Documentos clínicos electrónicos interoperados Ene 2020 – jul 2023

Documento Clínico	Sur	Sur Occidente	Norte	Centro Oriente
Consulta Externa <b>4,583,031</b>	1,477,669	765,261	1,623,007	717,094
Urgencias (Epicrisis) <b>636,850</b>	51,356	24,786	478,841	81,867
Hospitalización (Epicrisis) <b>304,513</b>	78,405	40,711	118,082	67,315
Odontología <b>531,357</b>	159,884	190,627	57,847	122,999
Imágenes DX <b>47,250</b>	43,563	3,666	17	4
Laboratorio Clínico <b>720,864</b>	41,241	39,548	640,075	0
Materno <b>149,431</b>	19,298	24,728	92,595	12,810

Fuente: Plataforma Bogotá Salud Digital – Modulo Informes – Corte: 01/01/2020 – 31/07/2023

**4** Subredes Integradas de Servicio de Salud Interoperando la Historia Clínica Electrónica Unificada del Distrito Capital



**89%** de interoperabilidad la Historia Clínica Electrónica Unificada del Distrito Capital

**6,973,296** de documentos clínicos electrónicos interoperados



Acceso a la Historia Clínica Electrónica Unificada en **116** sedes de la red.



# Principales retos y barreras

- > Establecer el **lenguaje común de intercambio**.
- > Falta de reglamentación de la ley 2015 de 2020 (Interoperabilidad de Historia Clínica en Colombia).
- > Establecer un **entorno de gobernanza** (Funcional y Técnico) que oriente la estrategia y la gestión de los Servicios Ciudadanos Digitales, que involucre a los grupos de interés en la toma de decisiones, definición de los focos estratégicos de acción y distribución eficiente de los recursos disponibles, que permita:
  - **Integrar los servicios ciudadanos digitales en los procesos asistenciales y administrativos** institucionales.
  - Evaluar y garantizar la **calidad y completitud del dato** de acuerdo con las **reglas de negocio** aplicables a cada ámbito y grupo de interés.
  - Aumentar el **uso y apropiación** por parte de los usuarios internos y externos.
  - Mejorar la **percepción del usuario** frente a los servicios ciudadanos digitales.





# Estándar de Interoperabilidad

- **HL7** (Health Level Seven): Conjunto de estándares globales para el intercambio de datos clínicos y administrativos de salud entre aplicaciones.
- **HL7 V2** (Versión 2 de HL7): Estándar de mensajería ampliamente implementado para el intercambio electrónico de datos clínicos en el dominio clínico. Posiblemente, el estándar más ampliamente implementado para la atención médica en el mundo.
- **HL7 CDA** (Clinical Document Architecture): Estándar de marcado de documentos desarrollado por HL7 International que especifica la estructura y semántica de los "documentos clínicos" para el intercambio entre proveedores de atención médica y pacientes.
- **HL7 FHIR** (Fast Healthcare Interoperability Resources): Estándar para el intercambio de datos de atención médica. FHIR es una especificación nueva basada en enfoques emergentes de la industria.
- **SNOMED** (Systematized Nomenclature of Medicine): Estándar internacional de terminología médica desarrollado por SNOMED International. Es el lenguaje común global más completo y preciso para los términos de salud en más de 50 países.
- **LOINC** (Logical Observation Identifiers Names and Codes): Base de datos y estándar universal para identificar observaciones de laboratorios médicos.



# Uso y apropiación

- La interoperabilidad se realiza de manera automatizada, no requiere intervención del profesional de salud.
- El acceso a la información se hace directamente desde el Sistema de Información Hospitalario de las Subredes.
- El distrito cuenta con un curso de capacitación a los profesionales de la salud, implementado por la SDS y liderado por cada Subred.



## ¿Medición?

Bogotá Salud Digital cuenta con un módulo dedicado a la generación de indicadores de operación e interoperabilidad, así como de indicadores de salud con base en la información interoperada.

## ¿Qué sigue?

Avanzar en la integración técnica y funcional de la Historia Clínica Electrónica Nacional con las IPS públicas y privadas de Bogotá, de la mano del Ministerio de Salud.

Interoperar la Historia Clínica Electrónica prehospitalaria y brindar acceso a los documentos clínicos electrónicos en tiempo real a los profesionales de la salud de las ambulancias, para mejorar la calidad de la atención y facilitar la toma de decisiones informadas.



# Gracias



SECRETARÍA DE  
SALUD





ALCALDÍA MAYOR  
DE BOGOTÁ D.C.

ALTA CONSEJERÍA  
DISTRITAL DE TIC

BOGOTÁ

COMPARTIC GOBIERNO  
Y SEGURIDAD  
DIGITAL  
BOGOTÁ

- Mejorando la eficiencia en los trámites y servicios al ciudadano con Interoperabilidad
- Interoperabilidad segura de datos personales

La **BOGOTÁ**  
que estamos construyendo





# ComparTIC



Conocer **cómo hacen otras** entidades **para mejorar la calidad** de vida de los ciudadanos



Aprender a utilizar la **tecnología como un medio** para facilitar el día a día de las ciudadanas y los ciudadanos



Implementar los lineamientos no es el objetivo final. Debemos **aprender a generar valor a partir de su implementación**

**Último martes de cada mes  
10:00 a.m. a 12:00 p.m.**

## Gobierno Digital

Mejorando la eficiencia en los trámites y servicios al ciudadano con interoperabilidad



Juan Gabriel Rubio  
Secretaría Distrital de Salud

## Seguridad Digital

Interoperabilidad segura de datos personales



David Vega  
Ágata

# Objetivo

- Presentar un caso de éxito de una entidad del distrito que ha logrado mejorar la eficiencia en sus trámites y servicios al ciudadano a través del uso de interoperabilidad. Se explorarán las técnicas y herramientas utilizadas para lograr esta mejora y se discutirá su impacto en la satisfacción del ciudadano. **Se presentará el caso de historia clínica electrónica por parte de la Secretaría de Salud de Bogotá.**
- Presentar recomendaciones prácticas de controles de seguridad esenciales para garantizar la protección de los datos personales cuando se comparten entre entidades. **Se presentarán recomendaciones técnicas por parte de Ágata Interoperabilidad segura de datos personales**



# Mensajes

## Concepto Interoperabilidad

---

- La interoperabilidad hace referencia a mecanismos y métodos que permiten a los sistemas de información interactuar e intercambiar datos de manera automática. En el marco del Gobierno digital, esta se orienta hacia la disminución de pasos en los trámites para la prestación de servicios al ciudadano y el aumento en la rapidez de la atención (implementación de cadenas de trámites). *(Conpes 3920 de 2018, Política Nacional de explotación Big Data)*

## Simplificación y mejora de experiencia de usuario

---

- La interoperabilidad es un factor indispensable para la simplificación y mejora de la experiencia del usuario, al permitir la integración de diferentes sistemas facilitando la interacción con los ciudadanos. Esto puede llevar a tiempos de respuesta más cortos y una prestación de servicios más eficiente en general.

## Protección de datos personales

---

- Aquellos datos que pertenezcan a ciudadanos y cuya pérdida y/o alteración pueda significar algún tipo de inconveniente para ellos con el Estado, deberán ser especialmente protegidos evitando el uso no autorizado y garantizando su integridad, disponibilidad y resguardo



# Formulación de la política pública

## Problemática

Insuficiencia de condiciones habilitadoras para que los actores del territorio aprovechen los datos, la tecnología y la innovación en la solución de problemáticas y desarrollo de oportunidades de mejora en el territorio.

## Objetivo general

Consolidar a Bogotá como un territorio inteligente impulsando el uso y aprovechamiento de los datos, la tecnología y la innovación, para la solución de problemáticas y la generación de oportunidades que mejoren la calidad de vida de las personas.

## Objetivos específicos

1. Cerrar la brecha digital ciudadana
2. Desarrollar competencias ciudadanas para territorio inteligente
3. Impulsar la adopción de tecnologías emergentes en el sector empresarial
4. Impulsar el aprovechamiento de los datos para la toma de decisiones
5. Consolidar la Innovación pública como dinamizador del territorio inteligente
6. Fortalecer capacidades para reducir riesgos y amenazas de seguridad digital.
7. Desarrollar un esquema de gobernanza de territorio inteligente para la Bogotá Región



# Gobierno Digital

Mejorando la eficiencia en  
los trámites y servicios al  
ciudadano con interoperabilidad



Juan Gabriel Rubio  
Secretaría Distrital de Salud

# Seguridad Digital

Interoperabilidad segura  
de datos personales



David Vega  
Ágata



# Calendario ComparTIC

Fecha	Tema Gobierno Digital	Tema Seguridad Digital
26 de septiembre	Creación de documentos digitales accesibles: Mejorando la experiencia para todos	Asegurando la integridad de los documentos digitales a través de firmas y certificados digitales
31 de octubre	Estrategias de Planeación de TI para una Transformación Digital Eficaz	Implementación exitosa de los Planes Estratégicos de Seguridad de la Información y los Planes de Tratamiento de Riesgos
21 de noviembre	Implementación de la Innovación en el Gobierno Distrital	Optimizando la privacidad y seguridad en la innovación
12 de diciembre	Mejorando la Conectividad Pública: Presentación de Programas Piloto y Cumplimiento del Acuerdo 855 de 2022	Conectividad distrital segura



ALTA CONSEJERÍA  
DISTRITAL DE TIC

**BOGOTÁ**



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.

ALTA CONSEJERÍA  
DISTRITAL DE TIC

**BOGOTÁ**

**2023**

## Alta Consejería Distrital de TIC

Secretaría General - Alcaldía Mayor de Bogotá

Tel: 601 3813000, ext. 2001

Bogotá, Colombia: Carrera 8 # 10 - 65

[tic.bogota.gov.co](http://tic.bogota.gov.co)



**@ConsejeriaTIC**

La **BOGOTÁ**  
que estamos construyendo

