REPÚBLICA DE COLOMBIA

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

RESOLUCIÓN NÚMERO 64454 DE 2021
(octubre 5 de 2021)

Por la cual se imparte una orden administrativa

VERSIÓN
ÚNICA

Radicación **21-321316**

LA DIRECTORA DE INVESTIGACIÓN DE PROTECCIÓN DE DATOS PERSONALES (E)

En ejercicio de sus facultades legales, en especial las conferidas por el artículo 19 y 21 de la Ley Estatutaria 1581 de 2012 y el artículo 17 del Decreto 4886 del 2011, y

CONSIDERANDO

PRIMERO. Que la Alcaldía Mayor del Distrito de Bogotá D.C.(la "Alcaldía Mayor" o "Alcaldía Mayor de Bogotá"), por intermedio de la Secretaría de Salud y el Fondo Financiero de Salud, como parte del Plan Ampliado de Inmunización ("PAI"), y con el fin de que los ciudadanos del distrito de Bogotá pudieran consultar su respectivo certificado de vacunación contra el virus pandémico Coronavirus 2019 ("COVID-19"), habilitó el aplicativo PAI 2.0. (el "Aplicativo") través del siguiente link de consulta: https://appb.saludcapital.gov.co/pai/publico/busqueda.aspx. De un estudio preliminar de ese aplicativo, realizado los días 11 y 12 de agosto de 2021[1], el Despacho evidenció lo siguiente:

1.1 Una vez se da click para ingresar a la plataforma de consulta de los certificados de vacunación se permite la consulta de la información para los siguientes tipos de personas (i) recién nacidos: donde se facilita la búsqueda por datos de identificación del recién nacido vacunado o datos de identificación de la madre ; (ii) menores: donde se permite la búsqueda por datos de identificación del menor vacunado o datos de identificación de la madre del menor, y; (iii) mayores: donde se puede realizar búsqueda con datos de identificación del vacunado. La consulta se encuentra protegida por un captcha para evitar la automatización en la búsqueda a través de bot o crawlers de minado de información.

Fuente:Página Frontal de la Plataforma de consulta.

[1] La evidencia de imágenes del aplicativo PAI 2.0 se realizó los días 11 y 12 de agosto de 2021, cuando el aplicativo estaba habilitado para consulta pública en el siguiente link: https://appb.saludcapital.gov.co/pai/publico/busqueda.aspx.

Fuente:Casilla de consulta para adultos donde se evidencia la consulta con el uso de CAPTACHA.

1.2 El Aplicativo carece de una Política de Tratamiento de Información (“PTI”) o un Aviso de Privacidad (“AP”) que permita a los titulares la finalidad del tratamiento y la entidad Responsable del Tratamiento información, más teniendo en cuenta que el aplicativo expone información sobre la salud de los titulares, como se muestra a continuación:

Fuente:Parte inferior del aplicativo donde se evidencia que carece PTI o AP específica.

Debe aclarse que la página de la Secretaría de Salud y el Fondo Financiero de Salud sí cuenta con dichas Políticas (http://www.saludcapital.gov.co/Documents/Politica_Proteccion_Datos_P.pdf), sin embargo, el aplicativo no remite a ellas. Esto quiere decir que si un ciudadano ingresa al aplicativo no tendrá forma de redirigirse a la (“PTI”) o a un (“AP”). Tampoco queda claro si la (“PTI”) dispuesta en la página de la Secretaría de Salud y el Fondo Financiero de Salud será la misma que rige al aplicativo PAI 2.0. o si, por el contrario, se dispone de una (“PTI”) independiente.

1.3 Una vez se realiza la consulta para una persona en específico, en este caso un adulto, se evidenció que arroja la siguiente información: (i) consecutivo; (ii) número de identificación, y; (iii) nombre completo. Sin embargo, se observó que el formulario arroja otros datos aplicables a menores recién nacidos o menores, tales como: (i) certificado de nacido vivo; (ii) tipo de documento de la madre; (iii) documento de la madre, y (iv) número de hijo.

Fuente:Consulta de una persona mayor para efectos de obtener el carné o certificado de vacunación.

1.4 Al descargar el certificado correspondiente a una persona mayor, se encontró, contrario a lo indicado[2] por parte de la Alcaldía Mayor[3], que el certificación de vacunación no solo es para la vacuna en contra del COVID-19, sino también para otras vacunas, tal como se pasa indicar a continuación:

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE SALUD

Institución vacunadora: Consulta Pública

Fecha de generación del carné: miércoles, 11 de agosto de 2021 06:55 p.m.

[redacted]

[redacted]

Escanee el código y obtenga su certificado digital de Vacunación COVID-19

Vacuna	Dosis	Fecha	Nombre comercial	Lote	Institución vacunadora
Anti - Rábica	Primera dosis				
	Segunda dosis				
	Tercera dosis				
	Cuarta dosis				
	Quinta dosis				
Antirrábica profiláctica	Primera dosis				
	Segunda dosis				
	Tercera dosis				
BCG	Única				
COVID - 19	Primera dosis				
	Segunda dosis				
	Única				
DPT	Única				
DPT Acelular	Segunda dosis	18/10/2016	Bostrix	AC37B177AB	UNIDAD DE SERVICIOS COMPENSAR AV 1 DE MAYO
Fiebre amarilla	Primera dosis				
	Refuerzo				
Fiebre tifoidea	Primera dosis				
	Segunda dosis				
Hepatitis A	Primera dosis				
	Segunda dosis				
Hepatitis A, Hepatitis B	Primera dosis				
	Segunda dosis				
	Tercera dosis				
Hepatitis B	Primera dosis				
	Segunda dosis				
	Tercera dosis				
	Refuerzo				

Fuente:Consulta de carné de vacunación generado en el aplicativo PAI.

1.5 Al descargar el documento correspondiente a una persona mayor, se comprobó, contrario a lo anunciado[4] por parte de la Alcaldía Mayor, que no solo se genera el certificado, sino el certificado de vacunación con la totalidad de las vacunas suministradas al Titular. Así mismo, dentro del documento se encuentra un código QR el cual permite, con su escaneó por parte de cualquier persona, el acceso al certificado de vacunación contra el COVID-19 de titular particular, así:

---

[2] Carolina Salazar Sierra, "Bogotá, la primera ciudad del país en habilitar certificado digital de vacunación Covid-19 (Ago. 12, 2021, 11:36 AM) en:https://www.larepublica.co/economia/bogota-la-primera-ciudad-del-pais-en-habilitar-certificado-digital-de-vacunacion-covid-19-3215608?utm_medium=Social&utm_source=Facebook&fbclid=IwAR2TxaW0xtbBgeOOm2FHPixJPXZ9IcEZpKsGc-08XpHtO3bXuwlE12yGJRc#Echobox=1628693516.(Se indicó lo siguiente: *"La Secretaría Distrital de Salud de Bogotá puso a disposición de la ciudadanía un aplicativo que permitirá generar un certificado digital de la vacunación contra el covid-19.De acuerdo con la entidad, esta medida se estableció con el fin de facilitar y garantizar el acceso a información veraz sobre la vacunación, evitando fraudes y adulteraciones"*).

[4] Carolina Salazar Sierra, "Bogotá, la primera ciudad del país en habilitar certificado digital de vacunación Covid-19 (Ago. 12, 2021, 11:36 AM) en:https://www.larepublica.co/economia/bogota-la-primera-ciudad-del-pais-en-habilitar-certificado-digital-de-vacunacion-covid-19-3215608?utm_medium=Social&utm_source=Facebook&fbclid=IwAR2TxaW0xtbBgeOOm2FHPixJPXZ9IcEZpKsGc-08XpHtO3bXuwlE12yGJRc#Echobox=1628693516.(Se indicó lo siguiente: *"La Secretaría Distrital de Salud de Bogotá puso a disposición de la ciudadanía un aplicativo que permitirá generar un certificado digital de la vacunación contra el covid-19.De acuerdo con la entidad, esta medida se estableció con el fin de facilitar y garantizar el acceso a información veraz sobre la vacunación, evitando fraudes y adulteraciones"*).

Fuente:Consulta del certificado de vacunación contra COVID – 19 – Bogotá generado del aplicativo PAI

1.6 Es necesario indicar que, a pesar de las medidas de seguridad tomadas por parte del distrito (i) Captcha, y; (ii) casilla de ingreso de información restringida; una vez arrojados los datos solicitados, estos pueden ser accedidos posteriormente a través de la consulta del historial del navegador y/o con la opción de cortado y pegado del sistema operativo de la URL;

1.7 La información que se trata a través de este aplicativo es la siguiente: (a) Para la consulta de mayores en el portal dispuesto se ingresan los datos de: (i)Tipo de persona, y (ii)Tipo de Identificación y Número; (b) Para la consulta de datos de menores en el portal dispuesto se ingresan los datos de: (i) Tipo de persona; (ii) Tipo de Identificación y Número, y; (iii) Datos e la madre, Tipo de identificación y Número. En relación a los datos de salud, se tienen acceso a los siguientes cuando el vacunado es mayor de edad: (i)Tipo de Identificación; (ii) número de identificación; (iii) nombres y apellidos, (iv) fecha de nacimiento; (v) Vacuna; (vi) dosis; (vii) fecha; (viii) nombre comercial; (ix) lote; (x) institución vacunadora. En relación con los menores de edad, se tiene acceso a los siguientes datos: (i) Tipo identificación; (ii) número de identificación – del vacunado y la madre; (ii) nombres y apellidos – del vacunado y la madre; (iii) fecha de nacimiento; (iv) Vacuna; (v) dosis; (vi) fecha; (vii) nombre comercial; (viii) lote; (ix) institución vacunadora.

SEGUNDO. En virtud de lo anterior, la Delegatura de Protección de Datos Personales de la Superintendencia de Industria y Comercio (“SIC”), mediante radicado 21-321316 - - 1 del 13 de agosto de 2021, requirió a la SECRETARÍA DE SALUD Y FONDO FINANCIERO DE SALUD, para que diera respuesta a los siguientes cuestionamientos:

> *1.¿Qué medidas de seguridad ha adoptado la Secretaría Distrital de Salud de Bogotá para impedir la adulteración, destrucción, pérdida, consulta, uso o accesos no autorizados o fraudulentos de los datos privados y sensibles relacionados con la información de las vacunas aplicadas a los ciudadanos?*
>
> *2. ¿Qué medidas de confidencialidad ha adoptado la Secretaría Distrital de Salud de Bogotá para garantizar la reserva de los datos privados y sensibles relacionados con las vacunas aplicadas a los ciudadanos?*
>
> *3. ¿Qué mecanismos técnicamente controlables ha adoptado la Secretaría Distrital de Salud de Bogotá para garantizar un conocimiento restringido de los datos privados y sensibles relacionados con la información de las vacunas aplicadas a los ciudadanos y evitar su disponibilidad en internet u otros medios de divulgación o comunicación masiva?*

2.1 De igual forma, el Despacho solicitó al equipo forense de esta entidad que realizara el respectivo análisis del aplicativo PAI, por lo que: (i) mediante radicado 21- 321316 - - 2 del 13 de agosto de 2021, se radicó el documento denominado “Análisis Técnico de Expedientes de la

Delegatura de Protección de Datos Personales – radicado 21- 321316" y sus anexos, y; (ii) mediante radicado 21-321316 - - 3 del 13 de agosto de 2021, se radicó el documento denominado "informe del aplicativo API".

Las conclusiones y comentarios más significativos de dichos informes fueron los siguientes:

- "Análisis Técnico de Expedientes de la Delegatura de Protección de Datos Personales – radicado 21- 321316" [5]:

Para el aplicativo WEB "**Aplicativo PAI 2.0**" de la url **https://appb.saludcapital.gov.co/pai/inicio/login.aspx**, donde se obtiene el carné de Vacunación de COVID-19 se encontró lo siguiente:

1. Para la consulta de mayores en el portal dispuesto se ingresan los datos de
   - Tipo de persona
   - Tipo de Identificación y Número

2. Para la consulta de datos de menores en el portal dispuesto se ingresan los datos de
   - Tipo de persona
   - Tipo de Identificación y Número
   - Datos e la madre, Tipo de identificación y Número.

3. Se puede acceder a los datos del vacunado mayor y de vacunas:
   - Tipo de Identificación
   - Número de Identificación
   - Nombres y apellidos
   - Fecha de nacimiento
   - Vacuna
   - Dosis
   - Fecha
   - Nombre comercial
   - Lote
   - Institución Vacunadora.

4. Cuando se consultan los datos de menores
   - Tipo de Identificación
   - Número de Identificación – Del vacunado y de la madre
   - Nombres y apellidos – Del vacunado y de la madre
   - Fecha de nacimiento
   - Vacuna
   - Dosis
   - Fecha
   - Nombre comercial
   - Lote
   - Institución Vacunadora.

[5] Comunicación No.21-321316, consecutivo 2.

5. Para acceder a la información realizando el paso a paso indicado en la página, se debe llenar un Código Captcha, si este es correcto se habilita acceso para consulta de la información.

6. Para acceder al carné de Vacunación de COVID-19, se debe hacer lectura de un código QR que dirige a una url con la información de titular Nombre, Vacuna, dosis, Laboratorio, fecha de aplicación, institución vacunadora, lote y vacunador, si no aparece el registro de vacunación de COVID-19 solo muestra el nombre completo del titular.

7. Cuando se realizan las consultas iniciales se producen URL de consulta para datos de vacunación y carné, en la URL se vincula un consecutivo por cada titular, este número se puede modificar en la URL de consulta y así acceder a la información de otros titulares mayores o menores de edad según las pruebas descritas en el acta.

8. Para acceder a la información de otros titulares con el cambio de ID desde la URL la página no solicita algún control como Código Captcha.

9. Se puede exportar la información de todas las consultas realizadas en varios formatos como PDF, CSV (delimitado por comas), entre otros.

10. En el proceso de consulta no se encontraron documentos, enlaces, textos relacionados con protección de datos o autorizaciones.

- "Informe del aplicativo API" [6]:

Análisis Funcional

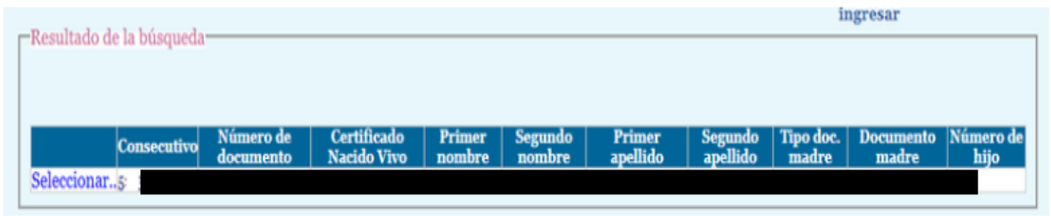
A continuación, se relacionan los hallazgos encontrados durante el proceso de análisis funcional de la opción "Consulte su carné de vacunación" que se encadena desde la página principal del aplicativo.

Por medio de esta opción un ciudadano puede generar un reporte de las vacunas que ha recibido, información que se muestra ingresando únicamente el tipo y número de documento de identificación para las consultas de adultos y tipo y numero de documento del menor y de la madre para los menores de edad.

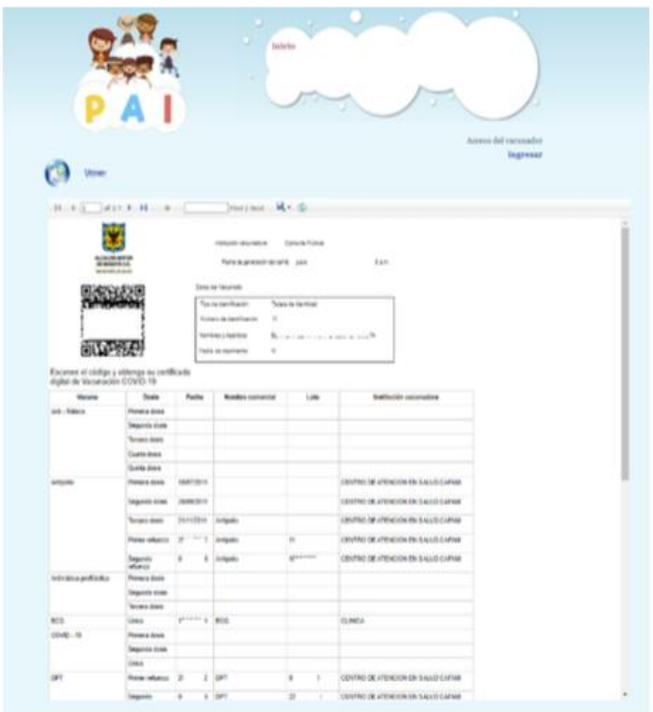
[6] Comunicación No. No.21-321316, consecutivo 3.

Para los casos de los menores de edad se requiere el número de identificación del menor y de la madre. El aplicativo no solicita el ingreso de un dato adicional al número de identificación para comprobar la titularidad de la persona que realiza la consulta y solo con el número de identificación muestra los datos relacionados.

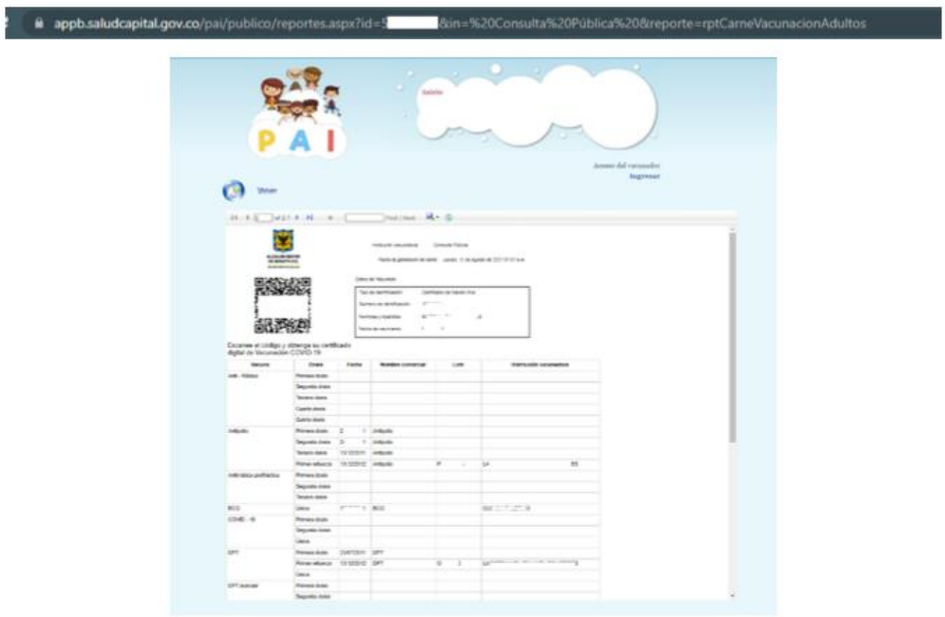
Luego de ingresar un captcha, se realiza la consulta y el sistema muestra los datos generales de la persona incluyendo nombre completo, número de identificación, certificado de nacido vivo y un "consecutivo".



Por medio del enlace "seleccionar" aparece un reporte con las vacunas aplicadas a la persona.



En esta opción el sistema muestra una URL en la cual se utiliza el parámetro "id" que corresponde al campo "consecutivo" de la pantalla anterior. Cambiando el valor de este parámetro, por números secuenciales mayores o menores, es posible acceder a la información de vacunación de otras personas, adultos o menores de edad.



Este reporte incluye opciones para descargar la información en diferentes formatos como: Excel, Pdf, Word, html; entre otras.

El código QR que muestra el reporte, encadena con otra opción del aplicativo que muestra los detalles de la vacunación aplicada para COVID-19.

Esta opción también hace uso del parámetro "id" que se puede cambiar en forma consecutiva para obtener información de otras personas.

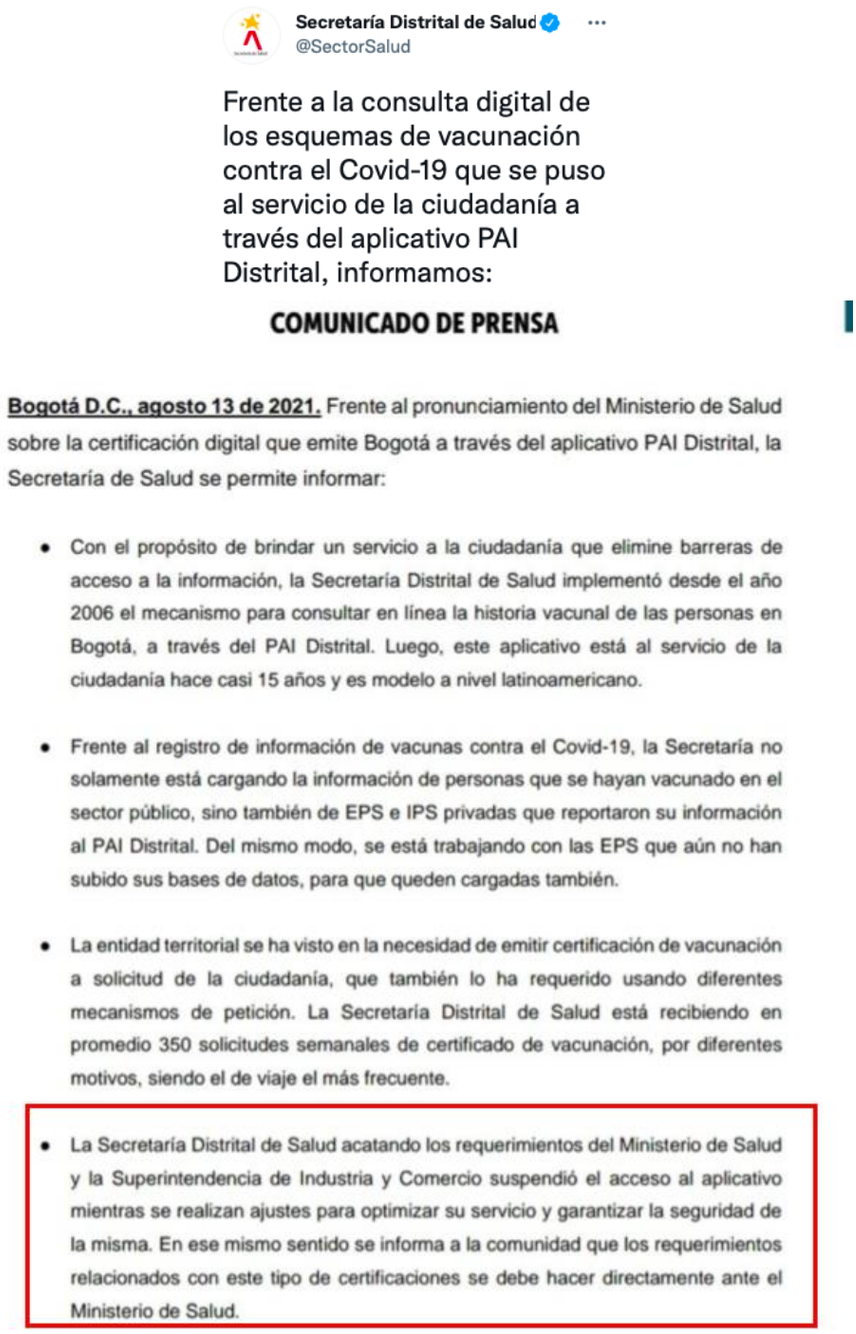
Conclusiones

La aplicación presenta fallas de seguridad y expone información sensible que puede ser consultada y descargada por terceras personas.

Se debe modificar la aplicación e implementar controles que permitan asegurar que se muestre únicamente la información correspondiente a la persona cuya identificación se ha validado previamente.

Se deben implementar mecanismos de seguridad para asegurar que la información se consulta únicamente por el titular y evitar que terceras personas puedan conocer estos datos solamente ingresando el número de identificación.

TERCERO. El 13 de agosto de 2021 la SECRETARÍA DE SALUD Y FONDO FINANCIERO DE SALUD emitió un comunicado de prensa en el que manifiesta que acatando los requerimientos del Ministerio de Salud y esta entidad "*suspendió el acceso al aplicativo mientras se realizan ajustes para optimizar su servicio y garantizar la seguridad de la misma*"[7]:



Secretaría Distrital de Salud
@SectorSalud

Frente a la consulta digital de los esquemas de vacunación contra el Covid-19 que se puso al servicio de la ciudadanía a través del aplicativo PAI Distrital, informamos:

COMUNICADO DE PRENSA

Bogotá D.C., agosto 13 de 2021. Frente al pronunciamiento del Ministerio de Salud sobre la certificación digital que emite Bogotá a través del aplicativo PAI Distrital, la Secretaría de Salud se permite informar:

- Con el propósito de brindar un servicio a la ciudadanía que elimine barreras de acceso a la información, la Secretaría Distrital de Salud implementó desde el año 2006 el mecanismo para consultar en línea la historia vacunal de las personas en Bogotá, a través del PAI Distrital. Luego, este aplicativo está al servicio de la ciudadanía hace casi 15 años y es modelo a nivel latinoamericano.

- Frente al registro de información de vacunas contra el Covid-19, la Secretaría no solamente está cargando la información de personas que se hayan vacunado en el sector público, sino también de EPS e IPS privadas que reportaron su información al PAI Distrital. Del mismo modo, se está trabajando con las EPS que aún no han subido sus bases de datos, para que queden cargadas también.

- La entidad territorial se ha visto en la necesidad de emitir certificación de vacunación a solicitud de la ciudadanía, que también lo ha requerido usando diferentes mecanismos de petición. La Secretaría Distrital de Salud está recibiendo en promedio 350 solicitudes semanales de certificado de vacunación, por diferentes motivos, siendo el de viaje el más frecuente.

- La Secretaría Distrital de Salud acatando los requerimientos del Ministerio de Salud y la Superintendencia de Industria y Comercio suspendió el acceso al aplicativo mientras se realizan ajustes para optimizar su servicio y garantizar la seguridad de la misma. En ese mismo sentido se informa a la comunidad que los requerimientos relacionados con este tipo de certificaciones se debe hacer directamente ante el Ministerio de Salud.

CUARTO. El 23 de agosto de 2021, la SECRETARÍA DE SALUD Y FONDO FINANCIERO DE SALUD contestó el requerimiento realizado por el Despacho, en el siguiente sentido[8]:

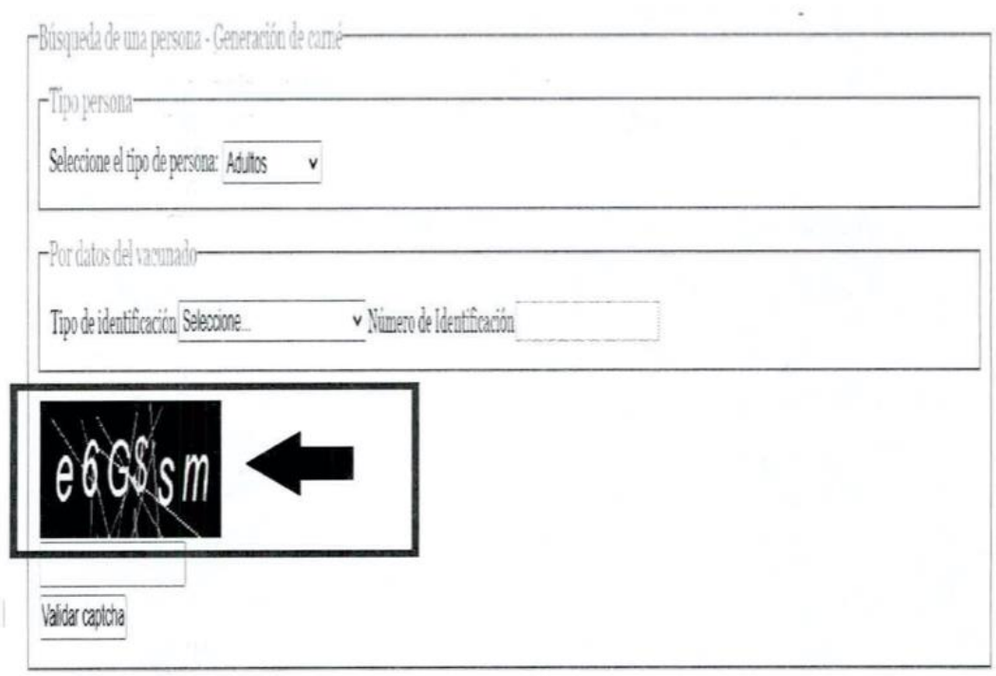
---

[7] Comunicado de prensa 13 de agosto de 2021. Secretaría Distrital de Salud. Disponible en: https://twitter.com/SectorSalud/status/1426195048471879680. (Consultado el 4 de octubre de 2021)
[8] Comunicación No. 21-321316, consecutivos 4, 5 y 6.

4.1. En primer lugar, informa que el “sistema de información “consulta certificado de vacunación COVID-19” fue puesto en operación el día 11 de agosto de 2021 y retirado el día 12 de agosto.

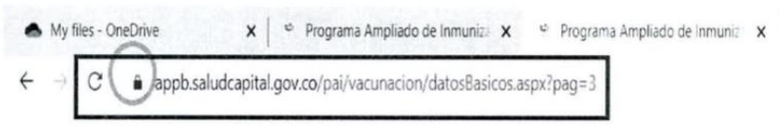
4.2. En relación con la primera pregunta realizada: *“¿Qué medidas de seguridad ha adoptado la Secretaría Distrital de Salud de Bogotá para impedir la adulteración, destrucción, pérdida, consulta, uso o accesos no autorizados o fraudulentos de los datos privados y sensibles relacionados con la información de las vacunas aplicadas a los ciudadanos?”,* mencionan lo siguiente:

> “*Como punto de partida es importante mencionar que a partir del año 2003 y ante la necesidad de conocer el registro vacunal de la población de Bogotá y realizar el seguimiento a la oportunidad y completitud del esquema de vacunación, se creó la herramienta tecnológica denominada Sistema Nominal de Información PAI, actualmente conocido como Sistema de Información PAI, el cual permite administrar, recolectar, procesar y almacenar la información relacionada con la vacunación de Bogotá D.C.*
>
> *Con el fin de impedir la adulteración, destrucción, pérdida, consulta, uso o acceso no autorizados o fraudulentos de los datos privados y sensibles relacionados con la información de las vacunas aplicadas a los ciudadanos, la Secretaria Distrital de Salud, implementó una funcionalidad únicamente de consulta de la información de vacunación y que cuenta con las siguientes medidas de seguridad:*
>
> *a. Validación captcha (funcionalidad para determinar si la solicitud es realizada por un humano y no una máquina), con el fin de evitar ataques por bots (máquina) y validaciones a nivel de dato, con el fin de minimizar riesgos por ataque de tipo "Cross Site Scripting", como se muestra en la siguiente imagen:*

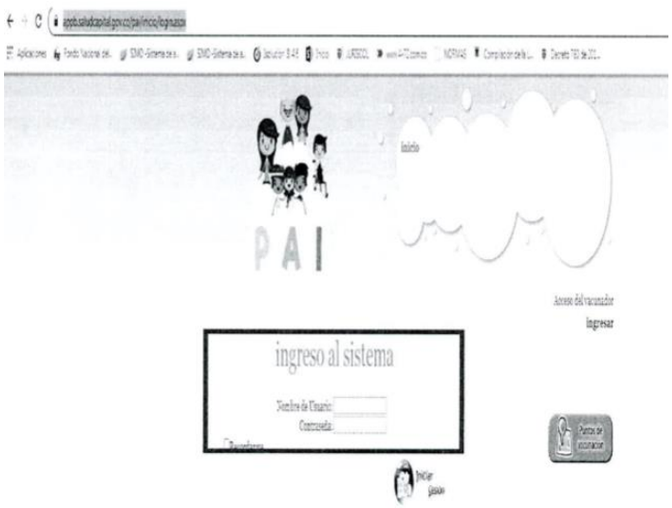


> *b. Servidor de aplicaciones con Internet Information Server - IIS, cuyo acceso se encuentra restringido. Únicamente pueden acceder a él los administradores del servidor y para ello, cuentan con un método de autenticación a través de una cuenta de usuario y contraseña. Además, el servidor cuenta con certificado de servidor seguro (SSL), el cual garantiza que la página web a la que se está conectando el*

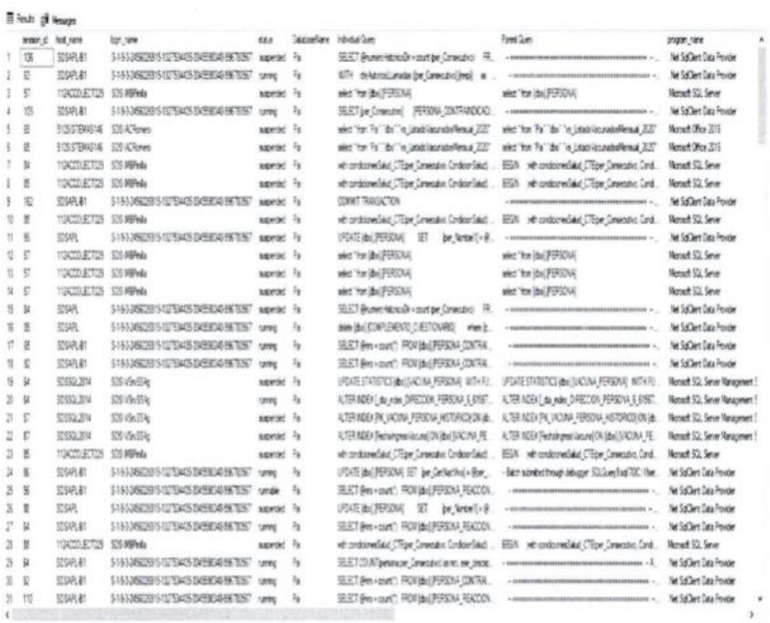
usuario para realizar la consulta (vacunas aplicadas), está siendo emitida por la Secretaría Distrital de Salud.
A modo de ejemplo en la siguiente imagen se muestra la disposición del certificado seguro. https://amb.saludcapital.gov.co/pai



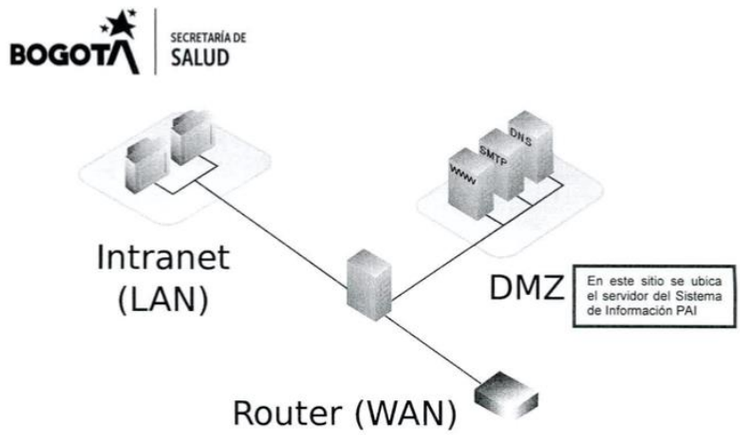
c. Acceso restringido a la información de los vacunados, a través de usuario y contraseña del personal autorizado, el cual es asignado por el administrador distrital del sistema de información. El registro y la consulta de la información solamente se puede realizar a través de la interfaz de usuario de la aplicación, teniendo en cuenta los niveles de acceso para cada rol:



d. Registro de eventos de acceso a la base de datos, que permite realizar actividades de auditoría para verificar las acciones realizadas sobre la información almacenada en la base de datos.



e. Servidor de bases de datos, el cual se encuentra en una zona de seguridad perimetral, que corresponde a la infraestructura tecnológica del servidor, la cual está configurada o parametrizada, con el fin de mitigar y contener diferentes ataques tecnológicos, lo cual impide accesos no autorizados a la información.



Las medidas de seguridad mencionadas anteriormente y desplegadas por la Secretaría Distrital de Salud garantizan el cumplimiento del principio rector de seguridad, consagrado en la Ley 1581 de 2012, manejando las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros, evitando así su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento."

4.3 Respecto a la segunda pregunta realizada: *¿Qué medidas de confidencialidad ha adoptado la Secretaría Distrital de Salud de Bogotá para garantizar la reserva de los datos privados y sensibles relacionados con las vacunas aplicadas a los ciudadanos?"* indican lo siguiente:

"*La información correspondiente al proceso de vacunación que se realiza por parte de los prestadores de servicios de salud a la población del Distrito Capital, se registra en el Sistema de Información PAI, independientemente del tipo de vacuna que se aplique. Este sistema de información opera desde hace más de quince (15) años, siendo fuente de consulta, especialmente para los siguientes eventos e instituciones, y que además cuenta con medidas de confidencialidad, como se verá más adelante:*

- *Cohorte de nacidos vivos en la ciudad de Bogotá. Esto significa que cada niño que nace en la ciudad, ingresa a este sistema de información con el inicio del esquema de vacunación.*
- *Entidades aseguradoras, para identificar la población que ha nacido y que pertenece a su entidad.*
- *Establecimientos educativos, con la finalidad de verificar que la población infantil, tenga su esquema de vacunación.*
- *Entidades territoriales, para determinar índices de vacunados en su población, en este caso en el Distrito Capital.*
- *El usuario, que requiere información al respecto.*

Desde el inicio de operación de la herramienta, se implementaron medidas de confidencialidad, como es el control de acceso y asignación de roles a los usuarios del sistema, es decir, administradores, vacunadores y usuarios de consulta, para seguimiento. Para cada rol, se establece una condición especial y diferente para el acceso a la información, por ejemplo:

- *El Administrador, tiene acceso a todas las funcionalidades del Sistema, en especial, la parametrización, creación, modificación o eliminación de usuarios.*
- *El Vacunador, tiene acceso al Sistema, para registrar los eventos de vacunación indicando la persona y la vacuna con sus detalles.*
- *El Usuario, únicamente podrá consultar las vacunas que le han sido administradas.*

Los roles descritos, representan el grado de confidencialidad con el que cuenta el Sistema, dado que, cada uno tiene limitaciones frente al acceso y manejo de la información.

Ahora bien, frente a los múltiples requerimientos de la población vacunada en Bogotá e interesada en realizar viajes al exterior, surgió la necesidad de crear una funcionalidad de consulta que permitiera presentar y validar la información de manera digital y en tiempo real, de los ciudadanos que lo requirieran.

Por esta razón, el día 11 de agosto de 2021 la Secretaría Distrital de Salud, habilitó esta consulta al servicio de los ciudadanos, la cual contiene los mismos parámetros de restricción, de un usuario de consulta, es decir, no puede registrar, modificar o eliminar ningún dato consignado en el Sistema.

Esta consulta dejó de operar el día 12 de agosto de 2021, producto de las observaciones recibidas por diferentes fuentes.

Con respecto a la confidencialidad de la consulta y los controles dispuestos, ésta presenta una información limitada de datos (nombre, documento de identidad y vacunas). De ninguna manera el Sistema presenta o permite observar información adicional, correspondiente a dirección, teléfono u otros datos identificadores de la persona.

Lo que se buscó con la funcionalidad de la consulta, fue justamente darle aplicabilidad a importantes disposiciones legales, que ubican la salud pública, como un elemento de primer orden, para la garantía de la salud en la comunidad y que ésta permita conocer y diseñar estrategias, para ampliar las oportunidades de vacunación en la población.

Por tanto es importante tener presente lo dispuesto en la Ley 9 de 1979 "Por la cual se dictan Medidas Sanitarias", que establece lo siguiente:

> *"Artículo 594°.- La salud es un bien de interés público."*
> *"Artículo 597°.- La presente y demás leyes, reglamentos y disposiciones relativas a la salud son de orden público.*"

4.4 Frente a la tercera pregunta realizada: ¿Qué mecanismos técnicamente controlables ha adoptado la Secretaría Distrital de Salud de Bogotá para garantizar un conocimiento restringido de los datos privados y sensibles relacionados con la información de las vacunas aplicadas a los ciudadanos y evitar su disponibilidad en internet u otros medios de divulgación o comunicación masiva?, mencionan lo siguiente:

"*Como se anotó en las respuestas a las preguntas 1 y 2, los mecanismos para garantizar un conocimiento restringido de los datos privados y sensibles relacionados*

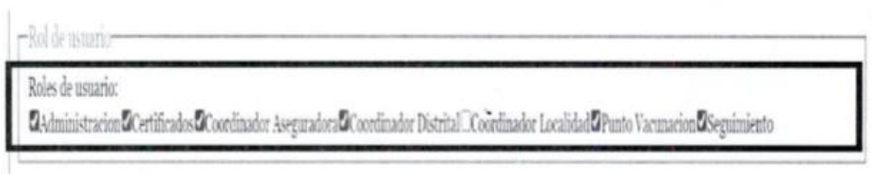
con la información que se registra en el sistema, requieren de la asignación de un rol, el cual, cuenta con limitaciones y permisos de acceso a la información.

Para este caso de la funcionalidad, se asignó un rol de consulta y datos determinados (nombre, documento de identidad y vacuna), el cual pudo ser consultado por internet, los días 11 y 12 de agosto, en la dirección URL previamente mencionada en el numeral 1."

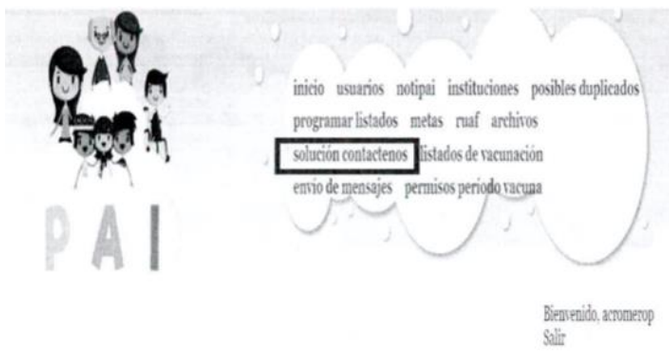
4.5 Además de lo anterior, se aporta la siguiente información:

"*El sistema PAI cuenta con:*

a. Autorización de ingreso al sistema: La información relacionada con la aplicación de las vacunas, solo puede ser ingresada al sistema de información PAI, por los vacunadores o registradores debidamente autorizados y capacitados por cada Entidad Administradora de Planes de Beneficios de Salud - EAPB. Igualmente pueden acceder al sistema los funcionarios del grupo PAI que hacen parte de la Subsecretaría de Salud Pública de esta Secretaría, para realizar actividades de verificación de la información.



b. Módulo de contáctenos, como mecanismo de soporte, para atender las solicitudes de las IPS, respecto de la corrección de errores de digitación de la información, las cuales son realizadas por el Técnico de Sistemas o el Profesional Especializado del equipo PAI, de esta Entidad, una vez el generador del error, entregue la evidencia, para que este sea subsanado en el Sistema.



c. Medida de confidencialidad, al tener como protocolo, brindar información del esquema de vacunación administrado en el Distrito Capital, al titular del registro o su representante."

QUINTO. Que frente al Tratamiento de datos personales realizado por la Alcaldía Mayor de Bogotá D.C. a través del aplicativo PAI localizado en la página web

https://appb.saludcapital.gov.co/pai/publico/busqueda.aspx, este Despacho, con el fin de dictar las órdenes administrativas a que den lugar, considera lo siguiente:

5.1 PERSONA JURÍDICA RESPONSABLE DEL TRATAMIENTO DE INFORMACIÓN EN EL CASO DEL APLICATIVO PAI.

Tanto el Responsable como Encargado del Tratamiento de la información deben ser personas naturales o jurídicas, de naturaleza pública y/o privada. En el caso en concreto, se evidencia que, dentro de la sección 7 de la PTI, la Secretaría de Salud y el Fondo Financiero de Salud fungen como Responsable y Encargado, lo cual contraría el Régimen de Protección de Datos Personales en tanto que dichas entidades no tienen personería jurídica.

De esta manera, a la luz de la definición de Responsable[9] y Encargado[10] dadas por la Ley Estatutaria 1581 de 2012, y las funciones otorgadas al Alcalde Mayor de Bogotá por parte del Decreto 131 de 2020[11] -modificado por el Decreto 134 de 2020-, en cumplimiento del Decreto 749 de 2020, es el Distrito de Bogotá D.C. quien funge como Responsable del Tratamiento. De este modo, y para efectos del presente acto administrativo, quien hace las veces de Responsable del Tratamiento, y, por tanto, sobre quien recae el cumplimiento de cualquier orden que aquí se imparta, será el Distrito de Bogotá D.C., a través de la Alcaldía Mayor de Bogotá.

5.2 CLASE DE DATOS PERSONALES TRATADOS EN EL APLICATIVO PAI.

De igual forma, es necesario identificar y hacer mención a los datos que están sujetos a Tratamiento por parte de la Alcaldía Mayor de Bogotá mediante el aplicativo PAI 2.0., el cual trata datos, para efectos del Decreto 1377 de 2013, artículo 3, considerados sensibles, entre los cuales se encuentra los datos relativos a la salud -datos sobre vacunación, dosis y fechas inmunización- de ciudadanos y de niños, niñas y adolescentes -considerados como recién nacidos y menores dentro de la aplicación-, y los cuales son sujetos de especial protección por parte del Régimen de Protección de Datos.

En ese sentido, se debe decir que, según la Ley Estatutaria 1581 de 2012, artículo 5, y el Decreto 1377 de 2013, artículo 3 (3), los datos relativos a la salud, tal como son el historial de vacunción de un Titular, son catalogados jurídicamente como datos sensibles. Este tipo de información hace referencia a aspectos íntimos de la persona, cuyo acceso no autorizado puede llevar a la discriminación o comprometer los derechos y libertades del Titular. Es así que, por regla general, el Tratamiento de estos datos es restrictivo y sólo se puede realizar bajo ciertas condiciones

---

[9] Corte Constitucional [C.C.] SentenciaC-748/11, M.P. Jorge Ignacio Pretelt Chaljub, Gaceta de la Corte Constitucional [G. C. C.] (Vol. n/d, p. 13) (Colom.) (*"El responsable del tratamiento es aquel que define los fines y medios esenciales para el tratamiento del dato, incluidos quienes fungen como fuente y usuario y los deberes que se le adscriben responden a los principios de la administración de datos y a los derechos –intimidad y habeas data- del titular del dato personal. El responsable del tratamiento es quien debe solicitar y conservar la autorización en la que conste el consentimiento expreso del titular para el tratamiento de sus datos, así como informar con claridad la finalidad del mismo.").*

[10] Ibídem, ("El encargado es aquel que debe *realiza del tratamiento de datos personales por cuenta del responsable del tratamiento, quien, en cumplimiento de los principios de libertad y finalidad, al recibir la delegación para tratar el dato en los términos en que lo determine el responsable, debe cerciorarse de que aquel tiene la autorización para su tratamiento y que el tratamiento se realizará para las finalidades informadas y aceptadas por el titular del dato. Si bien, en razón de la posición que cada uno de estos sujetos ocupa en las etapas del proceso del tratamiento del dato, es al responsable al que le corresponde obtener y conservar la autorización del titular, ello no impide al encargado solicitar a su mandante exhibir la autorización correspondiente y verificar que se cumpla la finalidad informada y aceptada por el titular de dato.")*

[11] D.131/20, art. 3: Con el fin de facilitar a la ciudadanía la acreditación del cumplimiento de una actividad económica y laboral exceptuada por el gobierno nacional, y obtener información que permita adoptar decisiones que reduzcan los riesgos de contagio y propagación de la epidemia del COVID-19 en la movilidad en Bogotá, D.C., las personas que deban movilizarse fuera de su domicilio para realizar actividades económicas y laborales, podrán acreditar por una vez a través del formulario previsto por la Alcaldía Mayor de Bogotá en la aplicación digital Gobierno Abierto de Bogotá – GABO- o en la página web www.bogota.gov.co/bogota-cuidadora la actividad económica y la principal forma de movilidad utilizada para adelantarla. La recolección de esta información tiene como objetivo organizar y optimizar formas de transporte bioseguras para la ciudadanía. Igualmente en la aplicación digital Gobierno Abierto de Bogotá – GABO- o en la página web www.bogota.gov.co/bogota-cuidadora los ciudadanos podrán solicitar su inclusión en alguno de los programas de apoyo social y económico que brinda la Administración Distrital, ofrecer ayuda a otros ciudadanos, y reportar sus síntomas y estado de salud. La información relacionada con estado de salud y síntomas se consolidará con la información recolectada por el gobierno nacional a través de CoronApp para estrictos efectos de cuidado epidemiológico, que reduzcan los riesgos de contagio y propagación de la epidemia del COVID-19. El suministro de cualquier información en la aplicación digital Gobierno Abierto de Bogotá – GABO- o en la página web www.bogota.gov.co/bogota-cuidadora es voluntaria y su tratamiento está sometida al principio de habeas data y a los mandatos establecidos para tal efecto en la Ley 1581 de 2012

indicadas en la Ley Estatutaria 1581 de 2012, el Decreto 1377 de 2013 y la jurisprudencia de la Corte Constitucional.

De esta manera, la Ley Estatutaria 1581 de 2012 en su artículo 6 determinó que los datos sensibles solo pueden ser tratados de manera restrictiva, razón por la cual, por mandato de la Corte Constitucional, a través del artículo 6 del Decreto 1377 de 2013, se establecieron los requisitos especiales para que el Titular del dato sensible otorgue su respectiva autorización para el Tratamiento por parte del Responsable.

En todo caso, en el Tratamiento de información sensible se le exige a los Responsables y/o Encargados actuar con una diligencia y cuidado reforzados, utilizando las mejores medidas -humanas, técnicas y administrativas- de seguridad para restringir el acceso, asegurar la confidencialidad, y la circulación de los datos personales sensibles, lo cual se traduce en una **Responsabilidad Reforzada** que conlleva al cumplimiento estricto de los principios y deberes consagrados por el Régimen de Protección de Datos a los Responsables Y/o Encargados.

En otras palabras, el tratamiento de datos sensibles debe estar rodeado de especial cuidado y diligencia en su recolección, uso, seguridad o cualquier otra actividad que se realice con los mismos. En efecto, la Corte Constitucional exige responsabilidad reforzada por parte de los Responsables y Encargados: "*como se trata de casos exceptuados y que, por tanto, pueden generar altos riesgos en términos de vulneración del habeas data, la intimidad e incluso la dignidad de los titulares de los datos,* ***los agentes que realizan en estos casos el tratamiento tienen una responsabilidad reforzada que se traduce en una exigencia mayor en términos de cumplimiento de los principios del artículo 4 y los deberes del título VI***"[12] (Énfasis añadido) . Por ende, los datos sensibles deben ser objeto de mayores medidas de seguridad, confidencialidad, circulación restringida y uso limitado.

Ahora como bien, para el Tratamiento de datos personales, como regla general, es necesaria la autorización previa, expresa e informada del Titular, que, tratándose de datos de naturaleza sesible, además de los requisitos generales, implica el cumplimiento de requisitos especiales establecidos en el artículo 12 de la Ley Estatutaria 1581 de 2012 y el artículo 6 del Decreto 1377 de 2013, así:

(i) Que el titular no está obligado a autorizar el Tratamiento de la información sensible;
(ii) Que los cuestionamientos que se le hagan sobre este tipo de datos sean facultativas;
(iii) Indicación expresa de cuáles son los datos que serán objeto del Tratamiento, y;
(iv) Finalidad del Tratamiento.

Una vez cumplido todo lo anterior, y teniendo en cuenta cuáles son las excepciones del Tratamiento de información sensible, es posible el Tratamiento de información.

Sin embargo, como ya se anotó, la información que se trata a través del aplicativo no es solo la sensible de titulares adultos, sino también de niños, niñas y adolescentes -considerados como recién nacidos y menores dentro de la aplicación-, por lo que será necesario tener en cuenta estrictamente el contenido del artículo 7 de la Ley Estatutaria 1581 de 2012, y el artículo 12 del Decreto 1377 de 2013, toda vez que, procurando el uso responsable de sus datos bajo parámetros igual o más estrictos que los que aplican en el Tratamiento de los de datos sensibles, se debe -teniendo en cuenta la prohibición general del art. 7-:

(i) Responder y respetar los derechos de estos sujetos de especial protección, y;
(ii) Que asegure sus derechos fundamentales.

---

[12] Cfr. Corte Constitucional, sentencia C-748 de 2011, numeral 2.8.4

Por su parte, conexo al Régimen de Protección de Datos Personales, el artículo 19 de la Ley 1571 de 2015, estableció la creación de un sistema único de información de salud que *"(. . .) integre los componentes demográficos, socioeconómicos, **epidemiológicos, clínicos**, administrativos y financieros."* (negrillas fuera del texto), lo cual conlleva la posibilidad del uso de los medios de la tecnología y la información para consulta, entre otros datos, de aquellos relacionados con el historial de vacunación como parte del componente epidemiológico y clínico de un titular, lo cual, en todo caso, y para todos los efectos, debe articularse con el contenido del Régimen de Protección de Datos Personales.

Respecto al acceso a la información sensible de salud de los titulares, la Corte Constitucional en sentencia C-311/14, a propósito de la constitucionalidad del proyecto de Ley Estatutaria del derecho fundamental a la salud -Ley 1751 de 2015, artículo 19-, determinó lo siguiente:

> *"De esta manera, un sistema único de información en salud para que cumpla con el fin esencial de garantía efectiva (art. 2 C.P.) del derecho fundamental no solo debe operar en línea entre los diferentes actores sino que debe generar reportes, alertas y datos suficientes en tiempo real, de manera que tanto los usuarios como las autoridades puedan obtener de manera oportuna el conocimiento de lo que acaece en el sector.*
>
> *Como se indicó, vulnera el derecho a la salud, en su dimensión de accesibilidad, que existan bases de datos fragmentadas o desactualizadas, al igual que la omisión de cualquier agente del sistema en cumplir con el deber de reportar los datos concernientes a su operación y su relación con los pacientes. (. . .)*
>
> *El uso eficiente de las tecnologías de la información no puede seguir estando ausente del sector salud. Todos los actores están obligados a suministrar información veraz e imparcial (art. 20 C.P.) (. . .) a través de las herramientas informáticas permita saber, en el mismo instante, el lugar, el sujeto que presenta una problemática sobre las cuales debe intervenirse para corregir y principalmente, para prevenir la ocurrencia de la vulneración del derecho a la salud.*
>
> *En este sentido, los datos en salud tienen una dimensión individual relacionada con el acto médico amparada por el derecho de habeas data y otra colectiva que garantiza, en el marco del acceso a la información pública, que se facilite el conocimiento de cuáles son los avances y retrocesos del sistema, las acciones de políticas pública adoptadas para superar los problemas y los resultados que con las medidas de regulación se obtengan."*[13]

En ese orden de ideas, es posible el Tratamiento de la información sensible de salud, incluyendo la relacionada con la epidemiológica y clínica -historial de vacunación- siempre que esta sea para: (i) Cumplimiento de la política de manejo de la información creada por la ley 1715 de 2015, y; (ii) Se sujete, en aquellos donde la información sea sensible, a los presupuestos del Régimen de Protección de Datos Personales.

En conclusión, se advierte que la información tratada a través del aplicativo PAI 2.0 por parte de la Alcaldía Mayor de Bogotá, como Responsable del Tratamiento, es de naturaleza sensible, cuya titularidad recae sobre ciudadanos mayores, niños, niñas y adolescentes; datos que deben sujetarse a las reglas estrictas para el Tratamiento establecidas en el Régimen de Protección de Datos Personales.

---

[13] Corte Constitucional [C.C.] SentenciaC-311/14, M.P. Gabriel Eduardo Mendoza Martelo, Gaceta de la Corte Constitucional [G. C. C.] (Vol. n/d, p. 25) (Colom.)

5.3 VULNERACIÓN AL PRINCIPIO DE SEGURIDAD (L.1581/12, art. 12(g)) Y EL DEBER DE MANTENER LA INFORMACIÓN BAJO CONDICIONES DE SEGURIDAD (L.1581/12, art 17(d)); EL PRINCIPIO DE CONFIDENCIALIDAD (L.1581/12, art. 12(h)) y EL PRINCIPIO DE ACCESO Y CIRCULACIÓN RESTRINGIDA(L.1581/12, art. 12(f))

En la Ley Estatutaria 1581 de 2012, artículo 4, literal (g) se establece el principio de rector de seguridad, el cual obliga a los Responsables a realizar el Tratamiento de la información bajo medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros, lo cual va aunado al deber del Responsable de conservar la información bajo condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento - artículo 17, literal (d), Ley Estatutaria 1581 de 2012-.

Al respecto, la Corte Constitucional ha determinado que:

> "(. . .) [E]l Responsable o Encargado del Tratamiento debe tomar las medidas acordes con el sistema de información correspondiente. Así, por ejemplo, en materia de redes sociales, empieza a presentarse una preocupación de establecer medidas de protección reforzadas, en razón al manejo de datos reservados. En el año 2009, el Grupo de Trabajo Sobre Protección de Datos de la Unión Europea señaló que en los 'Servicios de Redes Sociales' o 'SRS' debe protegerse la información del perfil en el usuario mediante el establecimiento de *'parámetros por defecto respetuosos de la intimidad y gratuitos que limiten el acceso a los contactos elegidos'*"[14]

De lo anterior debe entenderse que la norma busca establecer un elemento preventivo para que los Responsables, al igual que los Encargados, cuando sea el caso, adopten medidas necesarias, efectivas y demostrables, de carácter reforzado, para así evitar afectaciones a la seguridad de la información de los Titulares. El acceso, consulta y/o el uso no autorizado o fraudulento, así como la manipulación y pérdida de la información son los principales riesgos que se buscan mitigar a través de las medidas de seguridad de naturaleza humana, física, administrativas, técnicas y de cualquier otra índole que refuercen las anteriores medidas.

Igualmente, en virtud del principio de confidencialidad, la precitada Ley Estatutaria ordena que "*todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información*"[15]. Además, como manifestación del principio de acceso y circulación restringida, dicha Ley dispone que: "*Los datos personales, salvo la información pública, **no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley**"*[16]*.(Destacamos)*

En el caso en concreto, la Alcaldía Mayor de Bogotá, a través de la Secretaría de Salud y el Fondo Financiero de Salud, puso a disposición del público el aplicativo PAI 2.0. en la dirección URL: https://appb.saludcapital.gov.co/pai/inicio/login.aspx, donde se realiza recolección de información personal de los ciudadanos, tal como se indicó de 1.1. al 1.6. del considerando primero.

Por lo anterior, esta Dirección requirió a la Secretaría Distrital de Salud de Bogotá, para que, entre otras cosas, especificara qué medidas se seguridad, confidencialidad y de limitación de acceso y circulación había implementado para garantizar el debido Tratamiento de los datos

---

[14] Corte Constitucional [C.C.] SentenciaC-748/11, M.P. Jorge Ignacio Pretelt Chaljub, Gaceta de la Corte Constitucional [G. C. C.] (Vol. n/d, p. 40) (Colom.) (Interpreta el principio de Seguridad de la L.1581/12, y establece su alcance en la sección 2.6.5.2.7.).
[15] Cfr. Literal h) del artículo 4 de la Ley Estatutaria 1581 de 2012
[16] Cfr. Inciso segundo del Literal f) del artículo 4 de la Ley Estatutaria 1581 de 2012

personales recolectados, almacenados y Tratados a través del aplicativo PAI 2.0. A continuación, se extraen algunos de los apartados de esa respuesta:

A la pregunta de "¿Qué medidas de seguridad ha adoptado la Secretaría Distrital de Salud de Bogotá para impedir la adulteración, destrucción, pérdida, consulta, uso o accesos no autorizados o fraudulentos de los datos privados y sensibles relacionados con la información de las vacunas aplicadas a los ciudadanos?" la Secretaría contestó lo siguiente:

> *"La Secretaria Distrital de Salud, implementó una funcionalidad únicamente de consulta de la información de vacunación y que cuenta con las siguientes medidas de seguridad: (i) Validación captcha (funcionalidad para determinar si la solicitud es realizada por un humano y no una máquina), (…); (ii) Servidor de aplicaciones con Internet Information Server - IIS, cuyo acceso se encuentra restringido.(…) (iii) Acceso restringido a la información de los vacunados, a través de usuario y contraseña del personal autorizado, (…). (iv) Registro de eventos de acceso a la base de datos, (..) (v) Servidor de bases de datos, el cual se encuentra en una zona de seguridad perimetral (…)"*[17]

Añade que "las medidas de seguridad mencionadas anteriormente y desplegadas por la Secretaría Distrital de Salud garantizan el cumplimiento del principio rector de seguridad, consagrado en la Ley 1581 de 2012, manejando las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros, evitando así su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento"[18]*.*

Respecto a la segunda pregunta realizada: *¿Qué medidas de confidencialidad ha adoptado la Secretaría Distrital de Salud de Bogotá para garantizar la reserva de los datos privados y sensibles relacionados con las vacunas aplicadas a los ciudadanos?"* la Secretaría contestó lo siguiente:

> "*La información correspondiente al proceso de vacunación que se realiza por parte de los prestadores de servicios de salud a la población del Distrito Capital, se registra en el Sistema de Información PAI, independientemente del tipo de vacuna que se aplique. Este sistema de información opera desde hace más de quince (15) años, siendo fuente de consulta, especialmente para los siguientes eventos e instituciones, y que además cuenta con medidas de confidencialidad, (…) como es el control de acceso y asignación de roles a los usuarios del sistema, es decir, administradores, vacunadores y usuarios de consulta, para seguimiento.*
>
> *Para cada rol, se establece una condición especial y diferente para el acceso a la información, por ejemplo:*
>
> - *El Administrador, tiene acceso a todas las funcionalidades del Sistema, en especial, la parametrización, creación, modificación o eliminación de usuarios.*
> - *El Vacunador, tiene acceso al Sistema, para registrar los eventos de vacunación indicando la persona y la vacuna con sus detalles.*
> - *El Usuario, únicamente podrá consultar las vacunas que le han sido administradas.*

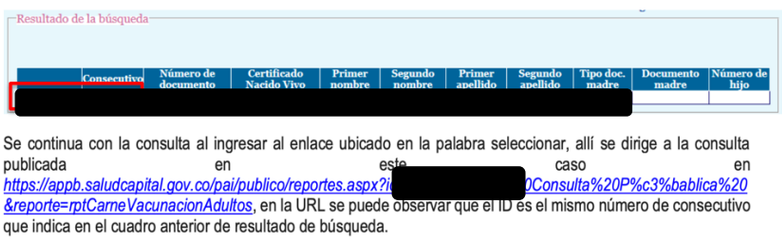
[17] Comunicación No.21-321316, consecutivos 4, 5 y 6.
[18] Ibídem.

> *Ahora bien, frente a los múltiples requerimientos de la población vacunada en Bogotá e interesada en realizar viajes al exterior,* ***surgió la necesidad de crear una funcionalidad de consulta que permitiera presentar y validar la información de manera digital y en tiempo real, de los ciudadanos que lo requirieran.*** *(…)*
>
> ***Con respecto a la confidencialidad de la consulta y los controles dispuestos, ésta presenta una información limitada de datos (nombre, documento de identidad y vacunas)****. De ninguna manera el Sistema presenta o permite observar información adicional, correspondiente a dirección, teléfono u otros datos identificadores de la persona. (…)*
>
> *Esta consulta dejó de operar el día 12 de agosto de 2021, producto de las observaciones recibidas por diferentes fuentes."*[19] *(Destacamos)*

Dicho lo anterior, esta Dirección encuentra que, a pesar de las medidas adoptadas por parte de la Alcaldía Mayor de Bogotá, a través de la Secretaría de Salud y el Fondo Financiero de Salud, para garantizar la seguridad, confidencialidad y acceso y circulación restringida de la información de vacunación de los ciudadanos, dichas medidas fueron ineficaces, insuficientes e inútiles porque no lograron garantizar la seguridad, la confidencialidad y el acceso restringido de la información personal de los ciudadanos -adultos y niños/niñas y adolescentes- recolectada, almacenada y Tratada en el aplicativo PAI 2.0.

En efecto, según en el documento denominado "Análisis Técnico de Expediente de la Delegatura de Protección de Datos Personales" ("análisis técnico")[20], esta Dirección comprobó técnicamente que, a pesar de que el acceso al aplicativo se encuentra restringido para su ingreso a través Captcha, restringiendo la automatización en la consulta, una vez se obtiene el resultado de consulta, se arroja el siguiente resultado tanto para adultos como para menores sin restricción alguna, así:

(a) Adulto



Se continua con la consulta al ingresar al enlace ubicado en la palabra seleccionar, allí se dirige a la consulta publicada en este caso en https://appb.saludcapital.gov.co/pai/publico/reportes.aspx?i[redacted]0Consulta%20P%c3%bablica%20&reporte=rptCarneVacunacionAdultos, en la URL se puede observar que el ID es el mismo número de consecutivo que indica en el cuadro anterior de resultado de búsqueda.

(b) Menores

Resultado de la búsqueda indica los datos del menor de edad y su consecutivo en este caso [redacted]

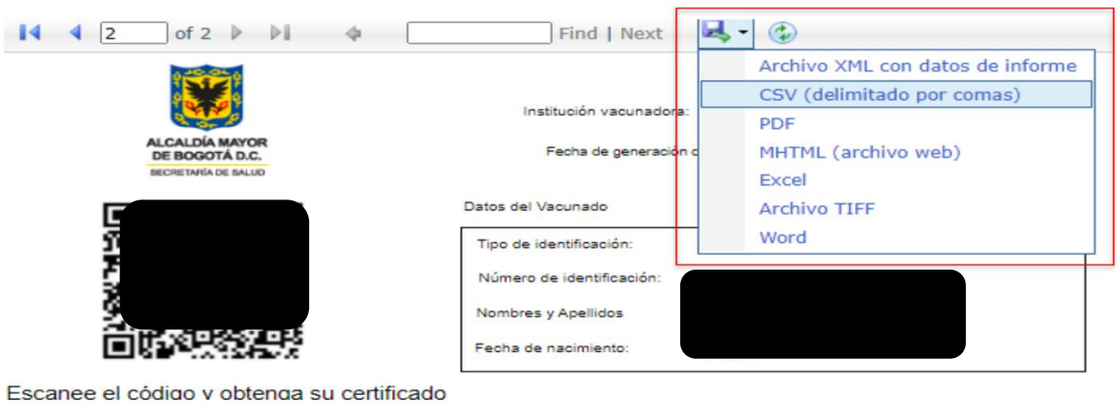
Datos del Vacunado, muestra datos del menor de edad y de la madre.

https://appb.saludcapital.gov.co/pai/publico/reportes.aspx?id=[redacted]n=%20Consulta%20P%c3%bablica%20&reporte=rptCarneVacunacionMenores

[19] Ibídem
[20] Comunicación No. 21-321316, consecutico 2.

En cada caso, se arroja una misma URL pero con variación en el consecutivo que resulta el parámetro clave para realizar la búsqueda por cada Titular independientemente, pudiendo en cada consulta acceder a otros datos tales como, en el caso de adultos, el número de hijos; y en el caso de menores, el número de certificado de nacido vivo, número de cédula de la madre, incluso la posición que tiene en la familia como hijo.

Como se indicó en el considerando 1.4., una vez se hace click en el botón de información, se arroja el carné de vacunación, el cual incluye la información de esquema de vacunación para distintos tipos virus y patologías, incluyendo el esquema en contra del COVID-19; donde también se incluye información relacionada con la IPS que realizó la vacunación respectiva. Respecto del Carné de vacunación, el análisis técnico indicó lo siguiente en relación a los formatos de exportación del mismo: *"Cuando se ingresa a los datos del vacunado se puede observar la opción para exportar la información de los titulares así:"*



Lo anterior muestra la posibilidad de exportar un formato editable del carné que puede ser modificado y parametrizado (archivos XML, Excel, y Word) para consultas posteriores y posiblemente modificado por parte de terceros con otros fines.

Por otra parte, el mismo formato de carné incluye un código QR que permite a los titulares escanearlo y obtener el certificado de vacunación contra COVID-19. Frente al particular, el análisis técnico indicó lo siguiente:

> *"Al escanear el código QR se genera el* ***Certificado de vacunación contra COVID-19*** *https://appb.saludcapital.gov.co/pai/publico/validacionCarne.aspx?id, nuevamente se observa el consecutivo dado por el sistema para la consulta de los datos del titular."*[21] Nótese nuevamente que el elemento clave para la consulta es el consecutivo asignado a cada titular -adultos y menores-, y a lo cual, al ser sujeto de pruebas de acceso por parte del equipo del forense de la SIC, se concluyó lo siguiente: *"Se toman las URL generadas en las consultas previas (datos de vacunación y carné), cambiando los consecutivos en el navegador y se obtiene acceso a la información de otros titulares, para su acceso no se requiere validar con Capcha como se realizó para el acceso inicial, o escanear el código QR, solo es suficiente cambiar el número de ID de las dos URL generadas en el proceso inicial para acceder a la información de otros titulares (. . .)".*[22]

[21] Radicado 21-321316 - - 2 del 13 de agosto de 2021. p.6.
[22] Ibidem, p. 10.

Para el efecto, se debe entender que las siguientes URL son los “portales” sobre la cual se hace la consulta en la base de datos una vez se obtiene y se ingresa el número de ID o consecutivo para cada titular:

https://appb.saludcapital.gov.co/pai/publico/validacionCarne.aspx?id**=(id específico asignador cualquier titular)**

https://appb.saludcapital.gov.co/pai/publico/reportes.aspx?id==**(id específico asignador a titular adulto)**&in=%20Consulta%20Pública%20&reporte=rptCarneVacunacionAdulto

https://appb.saludcapital.gov.co/pai/publico/reportes.aspx?id=**(id específico asignador a titular menor)**&in=%20Consulta%20P%c3%bablica%20&
reporte=rptCarneVacunacionMenores

De modo que, sin necesidad de ejecutar todo el procedimiento de seguridad a través el CAPTCHA, es posible, teniendo de antemano el número ID o consecutivo asignado a cada titular -adulto o menor-, obtener los datos de vacunación de cualquier ciudadano con historial de vacunación en el Distrito, el cual puede ser sujeto a modificaciones puesto que permite ser descargados en una amplia gama de formatos editables.

En igual sentido, es posible acceder al certificado de vacunación en contra del COVID-19. Así, tanto el carné de vacunación, como el certificado, pueden ser consultados de forma automatizada a través de un bot o crawler, para lo cual se requería los número de ID o consecutivo asignado para cada titular, los cuales pueden ser fácilmente adquiridos a través de un generador de números al azar que funcione dentro del patrón de números secuenciales que el Distrito le asignó a cada titular con esquema de vacunaciones aplicadas en la ciudad.

A lo anteriormente expuesto se le debe sumar las conclusiones del documento denominado “Análisis Aplicación PAI”, que fueron citadas anteriormente, y que se vuelven a poner de presente:

> *“(i) La aplicación presenta fallas de seguridad y expone información sensible que puede ser consultada y descargada por terceras personas; (ii) Se debe modificar la aplicación e implementar controles que permitan asegurar que se muestre únicamente la información correspondiente a la persona cuya identificación se ha validado previamente, y; (iii) Se deben implementar mecanismos de seguridad para asegurar que la información se consulta únicamente por el titular y evitar que terceras personas puedan conocer estos datos solamente ingresando el número de identificación.”*[23] Así mismo, el Informe Técnico en su parte final indicó, así como lo advirtió el Despacho en el análisis preliminar del aplicativo PAI, *“En el proceso de consulta no se encontraron documentos, enlaces, textos relacionados con protección de datos o autorizaciones.”*[24], lo que evidencia una ausencia de mecanismos administrativs concretos para la protección de datos de personales sensibles de vacunación por parte de la Alcaldía Mayor de Bogotá.

En ese orden de ideas, si bien es permitido el Tratamiento de datos sensibles en el ámbito de control epidemiológico y clínico de los Titulares, éste debe realizarse correctamente. En el caso concreto, las graves falencias detectadas en el aplicativo PAI 2.0 resultan incompatibles con los

[23] Radicado 21-321316 - - 3 del 13 de agosto de 2020. p.5.
[24] Radicado 21-321316 - - 2 del 13 de agosto de 2020. p.22.

mandatos de seguridad, confidencialidad y acceso y circulación restringida de la información personal establecidos por la Ley Estatutaria 1581 de 2012, toda vez que:

(i) El Tratamiento de los datos sensibles relativos a la vacunación de los ciudadanos no fue sujeto a las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros de vacunación, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento por parte de terceros;
(ii) Hubo ausencia de adopción de medidas de seguridad efectivas, demostrables y reforzadas para evitar la afectación a la seguridad de la información sensible de los titulares, más aún teniendo en cuenta que dentro del conjunto de datos tratados se encuentran los de niños, niñas y adolescentes.
(iii) No se garantizó la reserva de la información relativa a la vacunación de los ciudadanos.
(iv) No se evitó la disponibilidad en internet y otros medios de divulgación o comunicación masiva de dichos datos.
(v) No se dispuso de medidas de acceso técnicamente controlables para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados.

Ahora bien, el 13 de agosto de 2021 la SECRETARÍA DE SALUD Y FONDO FINANCIERO DE SALUD emitió un comunicado de prensa en el que, en otras cosas, se mencionaba lo siguiente [25]: *"La secretaría Distrital de Salud acatando los requerimientos del Ministerio de Salud y la Superintendencia de Industria y Comercio* ***suspendió el acceso*** *al aplicativo mientras se realizan ajustes para optimizar su servicio y garantizar la seguridad de la misma (…)"* (Destacamos).

En efecto, al consultar el sitio web de la aplicación PAI (https://appb.saludcapital.gov.co/pai/publico/busqueda.aspx)[26], se evidencia que la función de consulta para los ciudadanos -consulta pública- fue inhabilitada y que, en consecuencia, solo pueden ingresar los usuarios autorizados a través de un "Usuario" y una "Contraseña", como se muestra a continuación:

Considerando lo anterior, la Alcaldía Mayor de Bogotá, en su calidad de Responsable del Tratamiento de la información, debe adoptar medidas técnicas, humanas, administrativas de seguridad, confidencialidad y acceso y circulación restringida de la información personal de los Titulares registrados en la aplicación PAI 2.0. Dichas medidas deben ser necesarias, útiles, apropiadas, efectivas, eficientes, oportunas y demotrables para garantizar el derecho a la protección de Datos de los ciudadanos,

---

[25] Comunicado de prensa 13 de agosto de 2021. Secretaría Distrital de Salud. Disponible en: https://twitter.com/SectorSalud/status/1426195048471879680. (Consultado el 4 de octubre de 2021)
[26] Consulta realizada el 4 de octubre de 2021.

La adopción de estas medidas resulta muy relevante en el supuesto de que la función de "Consulta" de ese aplicativo se vuelva a habilitar y, en todo caso, siempre que se desarrollen nuevas aplicaciones o tecnologías en las que se realice Tratamiento de la información personal de los ciudadanos.

A continuación, la enunciación de algunas recomendaciones que, entre otras, resultan de importante consideración a la hora de garantizar, en la práctica, el efectivo derecho de Habeas Data de los ciudadanos:

En caso de que la función de "Consulta" -Consulta pública- se vuelva a habilitar en el aplicativo PAI 2.0, se recomienda tener en cuenta las siguientes sugerencias:

(a) Remover, para efectos del certificado de vacunación generado por el aplicativo, la opción de descarga a través de diversos formatos editables, y, en cambio, debe procederse a implementar un mecanismo de generación de un un único archivo en formato PDF no editable que sea solo sea para acceso de los titulares;

(b) Implementar dentro de cada certificado digital de vacunación, y para efectos del certificado de vacunación contra el COVID-19, el mecanismo de QR cifrado para evitar la consulta no autorizada o fraudulenta de los datos de vacunación de los titulares;

(c) Incorporar, en relación con los datos de vacunación de niños, niñas y adolescentes, y teniendo en cuenta que son sujetos de especial protección por el Régimen de Protección de Datos, un mecanismo de consulta donde se garantice que el representante legal de éstos sea el único que pueda tener acceso a los datos personales sensibles de los de niños, niñas y adolescentes.

Recomendaciones generales para cualquier desarrollo tecnológico o de cualquier índole, incluido el aplicativo PAI 2.0, en el que se realice Tratamiento de datos personales:

(d) Acoger en la totalidad del aplicativo PAI 2.0, en especial en la función de "Consulta" en caso de que ésta se vuelva a habilitar, y en cualquier otro desarrollo tecnológico o de cualquier índole en el que se realice Tratamiento de Datos Personales, el protocolo https -hyper Text Protocol Secure- que permita la encriptación de los datos personales sensibles y el cifrado del ID o consecutivo asignado a cada Titular.

(e) Incorporar en el aplicativo PAI 2.0, en especial en la función de "Consulta" en caso de que ésta se vuelva a habilitar, y en cualquier otro desarrollo tecnológico o de cualquier índole en el que se realice Tratamiento de Datos Personales, como parte de las medidas de seguridad administrativas, un Aviso de Privacidad que contengan como mínimo el lenguaje requerido por el artículo 15 del Decreto 1377 de 2013, así como el artículo 6 del Decreto 1377 de 2013 para efectos de datos sensibles, y el artículo 12 de la misma reglamentación para efecto de los niños, niñas y adolescentes.

(f) Adoptar en el aplicativo PAI 2.0, en especial en la función de "Consulta" en caso de que ésta se vuelva a habilitar, y en cualquier otro desarrollo tecnológico o de cualquier índole en el que se realice Tratamiento de Datos Personales, como parte de las medidas de confidencialidad y acceso y circulación restringida de la información, medidas y/o mecanismos de acceso técnicamente controlables que garanticen un conocimiento restringido de la información, esto es, sólo a los Titulares o terceros autorizados conforme a lo establece el párrafo segundo del literal f) de la Ley Estatutaria 1581 de 2012.

(g) Aplicar medidas y/o mecanismos que garanticen la estricta reserva de la información personal que sea tratada a través del aplicativo PAI 2.0, en especial en la función de "Consulta" en caso de que ésta se vuelva a habilitar, o cualquier otro desarrollo tecnológico o de cualquier índole en el que se realice Tratamiento de Datos Personales -*literal h) de la Ley Estatutaria 1581 de 2012*-.

Dado que la Alcaldía Mayor de Bogotá utilizó una herramienta tecnológica respecto de la cual se detectaron fallas de seguridad y de confidencialidad de información sensible, se considera relevante referirnos a la necesidad de adoptar medidas preventivas para evitar la vulneración de los derechos de las personas e incumplimientos de la regulación sobre Tratamiento de datos personales. A continuación, su desarrollo:

5.4 PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO PARA EL APLICATIVO PAI 2.0 Y CUALQUIER OTRO DESARROLLO QUE SE PRETENDA HABILITAR EN EL FUTURO.

Esta Dirección debe hacer énfasis en la necesidad de que, antes del lanzamiento de aplicativos o el uso de tecnologías similares por medio de las que se realice Tratamiento de la información de los ciudadanos, se incorpore la Privacidad como principio y piedra angular dentro de los procesos de diseño, operación y gestión de dichos aplicativos o herramientas para lograr una protección integral en lo que a Protección de Datos Personales se refiere -***Privacidad desde el Diseño (PbD)***-.

Aunado a lo anterior, también es necesario que se adopten mecanismos que garanticen que se traten únicamente lo datos que sean necesarios, adecuados y pertinentes en relación con los fines del Tratamiento y se garantice que la extensión de dicho Tratamiento sea la estrictamente necesaria. Asimismo, el tiempo o periodo de conservación de los datos debe estar justificado objetivamente en la finalidad del Tratamiento -***Privacidad por Defecto (PDpD)-.***

Las anteriores prácticas hacen referencia a lo que se conoce como "*La Privacidad desde el Diseño y por Defecto*". Esta Superintendencia ha señalado que se trata de una buena práctica y que es: "*una medida proactiva para, entre otras, cumplir con el Principio de Responsabilidad Demostrada (Accountability)"*[27]*.* Adicionalmente, " *al introducir la privacidad desde el diseño, se busca garantizar el correcto Tratamiento de los datos utilizados en los proyectos que involucren recolección, uso o tratamiento de datos personales*."

Es importante precisar que, si bien en Colombia no está consagrada expresamente, la implementación de "*La Privacidad desde el Diseño y por Defecto*" como una obligación del Responsable del Tratamiento, su ejecución es una medida proactiva que coadyuva a dar cumplimiento al Principio de Responsabilidad Demostrada, del que se hablará en un acápite siguiente.

Así las cosas, y profundizando en estos conceptos, la Privacidad por Diseño "*promueve la visión de que el futuro de la privacidad no puede ser garantizado sólo por cumplir con los marcos regulatorios; más bien, idealmente el aseguramiento de la privacidad debe convertirse en el modo de operación predeterminado de una organización*"[28] Por eso, esta Superintendencia ha reconocido que: "*desde antes que se recolecte información y durante todo el ciclo de vida de la*

---

[27] Superintendencia de Industria y Comercio. Texto de Convocatoria:"Sandbox sobre Privacidad desde el Diseño y por Defecto en proyectos de Inteligencia Artificial", abril, 2021. Disponible en: https://www.sic.gov.co/sites/default/files/files/2021/150421%20Sandbox%20sobre%20privacidad%20desde%20el%20diseño%20y%20por%20defecto.pdf. Pág. 11.

[28] Cfr. Cavoukia, Ann. Privacidad por Diseño: Los 7 principios fundamentales. Disponible en: http://mediascope.nl/wp-content/uploads/2015/08/privacidad-por-dise%C3%B1o.pdf https://www.mediascope.es/wp-content/uploads/2016/10/privacidad-por-disen%CC%83o -1.pdf. Ana Brian Nougreres también explica este tema en su artículo de 2012 publicado en la Revista Internacional de Protección de Datos Personales (RIPDP) y titulado "La protección inte- ligente de los datos personales: Privacy by Design (PbD)". El texto puede consultarse en: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/ok6_-Ana-Brian-Nougreres_FINAL.pdf

misma, se deber[án] adoptar medidas preventivas de diversa naturaleza (tecnológica; organizacional; humana; procedimental; entre otras) con el objeto de evitar vulneraciones al debido tratamiento de los datos personales."[29]

Respecto a la Privacidad desde el Diseño, la Agencia Española de Protección de Datos AEPD, por medio de la "Guía de Privacidad desde el Diseño"[30] menciona que:

> "La privacidad desde el diseño (en adelante, PbD) implica utilizar un enfoque orientado a la **gestión del riesgo y de responsabilidad proactiva** para establecer estrategias que incorporen la protección de la privacidad a lo largo de todo el ciclo de vida del objeto (ya sea este un sistema, un producto hardware o software, un servicio o un proceso).
>
> Por ciclo de vida del objeto se entiende todas las etapas por las que atraviesa este, desde su concepción hasta su retirada, pasando por las fases de desarrollo, puesta en producción, operación, mantenimiento y retirada. Más aun, implica que se tengan en cuenta, no sólo la aplicación de medidas de protección de la privacidad en las etapas tempranas del proyecto, sino que además se contemplen también todos los procesos y prácticas de negocio involucrados en el tratamiento de datos asociado, logrando así una verdadera gobernanza de la gestión de los datos personales por parte de las organizaciones.
>
> **El objetivo último es que la protección de datos esté presente desde las primeras fases de desarrollo y no sea una capa añadida a un producto o sistema. La privacidad debe formar parte integral de la naturaleza de dicho producto o servicio**." (Destacamos)

En suma, se busca que desde antes de iniciar algún tipo de Tratamiento de la información y durante todo el ciclo de vida de dicho Tratamiento, se adopten medidas preventivas de diversa naturaleza (tecnológica; organizacional; humana; procedimental; entre otras) que sean efectivas, útiles, necesarias y demostrables y que granticen un debido Tratamiento de los datos personales de los ciudadanos.

Ahora bien, en lo que respecta a la Privacidad por Defecto, la Agencia Española de Protección de Datos AEPD, a través de la "Guía de Protección de Datos por Defecto"[31] ha establecido que "*una aplicación demostrable de la protección de datos por defecto se convierte en una de las medidas de responsabilidad proactiva (Responsabilidad Demostrada) que permite acreditar el cumplimiento de las obligaciones establecidas en la norma*".

Al respecto, el apartado 2 del artículo 25 del Reglamento General de Protección de Datos europeo -RGPD- señala lo siguiente:

> "El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean

---

[29] Superintendencia de Industria y Comercio. Texto de Convocatoria:"Sandbox sobre Privacidad desde el Diseño y por Defecto en proyectos de Inteligencia Artificial", abril, 2021. Disponible en: https://www.sic.gov.co/sites/default/files/files/2021/150421%20Sandbox%20sobre%20privacidad%20desde%20el%20diseño%20y%20por%20defecto.pdf. Pág. 12.

[30] Agencia Española de Protección de Datos -AEPD-. "Guía de Privacidad desde el Diseño", 2019. Disponible en: https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf

[31] Agencia Española de Protección de Datos -AEPD-. "Guía de Protección de Datos por Defecto". Disponible: https://www.aepd.es/sites/default/files/2020-10/guia-proteccion-datos-por-defecto.pdf

> necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas."

En relación con la anterior norma, la Autoridad Española indica que:

> "El RGPD exige del responsable una configuración por defecto de los tratamientos que sea respetuosa con los principios de protección de datos, abogando por un procesamiento mínimamente intrusivo: mínima cantidad de datos personales, mínima extensión del tratamiento, mínimo plazo de conservación y mínima accesibilidad a datos personales. Todo ello, además, sin que sea necesaria la intervención del interesado para garantizar que estos mínimos están establecidos. **De ahí que la PDpD no se limita a requisitos sobre el programas o dispositivos, sino que afecta también al propio diseño del tratamiento, con independencia del soporte en el que se desarrolle el mismo**." (Destacamos)

Debe resaltarse que las medidas de Privacidad desde el Diseño deben estar conectadas con las medidas de Privacidad por Defecto, pues la incorporación y ejecución de ambos enfoques es lo que garantizará una real aplicación del Principio de Responsabilidad Demostrada y un debido Tratamiento de los datos personales en cualquier tecnología o herramienta a través de la cual se realice dicho Tratamiento.

Volviendo al caso concreto, considerando que la función de "Consultas" del aplicativo PAI está suspendida, en caso de que se volviera a habilitar dicha función y, en el futuro, para cualquier otro desarrollo tecnológico o de cualquier índole que involucre Tratamiento de datos personales, es imperativo que la Alcaldía Mayor de Bogotá, a través de la Secretaría de Salud y el Fondo Financiero de Salud, o cualquier otra Secretaría o dependencia a su cargo, desde el Diseño de la aplicación o herramienta de que se trate y durante el desarrollo de la misma, incorpore mecanismos de Privacidad que garanticen, entre otros, los principios de seguridad, confidencialidad y acceso y circulación restringida de los datos personales de los ciudadanos, conforme a lo descrito en este acápite y lo establecido en la Ley Estatutaria 1581 de 2012.

5.5 INCUMPLIMIENTO DEL PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA AL NO CREAR POLÍTICAS ESPECÍFICAS APROPIADAS PARA CUMPLIR CON LAS OBLIGACIONES ESTABLECIDAS POR EL RÉGIMEN DE PROTECCIÓN DE DATOS EN MATERIA DE DATOS SENSIBLES.

La regulación colombiana le impone al Responsable del Tratamiento la responsabilidad de adoptar las medidas necesarias para cumplir la Ley Estatutaria 1581 de 2012 y sus normas reglamentarias. Esas medidas deben garantizar un cumplimiento real y concreto, no simbólico o formal (mera expedición de documentos, políticas, etc). De ahí que la implementación de "La Privacidad desde el Diseño y por Defecto" sea una arista de primera importancia para el cumplimiento de este deber. Al respecto, nuestra jurisprudencia ha determinado que "*existe un deber constitucional de administrar correctamente y de proteger los archivos y bases* [sic] *de datos* [sic] *que contengan información personal o socialmente relevante*" [32]

[32] Cfr. Corte Constitucional, sentencia T-227 de 2003.

Adicionalmente, es importante resaltar que los Responsables del Tratamiento de los Datos no se convierten en dueños de los mismos como consecuencia del almacenamiento en sus bases o archivos. En efecto, al ejercer únicamente la mera tenencia de la información, solo tienen a su cargo el deber de administrarla de manera correcta, apropiada y acertada. Por consiguiente, si los sujetos mencionados actúan con negligencia o dolo, la consecuencia directa sería la afectación de los derechos humanos y fundamentales de los Titulares de los Datos. En virtud de lo anterior, el Capítulo III del Decreto 1377 de 27 de junio de 2013 -incorporado en el Decreto 1074 de 2015- reglamenta algunos aspectos relacionados con el Principio de Responsabilidad Demostrada.

La Corte Constitucional ha destacado el deber de adoptar medidas para demostrar que se ha cumplido la regulación de Datos personales. En efecto, mediante la Sentencia C-32 de 2021 reconoció la existencia de la responsabilidad demostrada en los siguientes términos:

> *"219. El principio de responsabilidad demostrada, conocido en el derecho comparado como accountability en la protección de datos personales, es incorporado por la legislación interna por el Decreto 1377 de 2013, reglamentario de la Ley 1581 de 2013 (sic). El artículo 26 de esa normativa determina que los responsables del tratamiento de datos personales deberán demostrar, a petición de la Superintendencia de Industria y Comercio, entidad que obra como autoridad colombiana de protección de datos, que han implementado medidas apropiadas y efectivas para cumplir con las citadas normas jurídicas. Esto de manera proporcional a: (i) la naturaleza jurídica del responsable y, cuando sea el caso, su tamaño empresarial; (ii) la naturaleza de los datos personales objeto de tratamiento; (iii) el tipo de tratamiento; y (iv) los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares del dato personal. Con este fin, los responsables deben informar a la SIC acerca de los procedimientos usados para el tratamiento de datos. A esta medida se suma lo previsto en el artículo 27 ejusdem, que estipula la obligación del responsable de establecer políticas internas que garanticen: (i) la existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable; (ii) la adopción de mecanismos internos para poner en práctica dichas políticas; y (iii) la previsión de procesos para la atención y respuesta a consultas, peticiones y reclamos de los titulares, respecto de cualquier aspecto del tratamiento de datos personales.*
>
> *El principio de responsabilidad demostrada, de acuerdo con lo expuesto, consiste en el deber jurídico del responsable del tratamiento de demostrar ante la autoridad de datos que cuenta con la institucionalidad y los procedimientos para garantizar las distintas garantías del derecho al habeas data, en especial, la vigencia del principio de libertad y las facultades de conocimiento, actualización y rectificación del dato personal"*[33].

En efecto, el artículo 26 de dicho Decreto [34]-*Demostración*- establece que, "*los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la*

---

[33] Cfr. Corte Constitucional, sentencia C-032 del 18 de febrero de 2021. M.P. Dra Gloria Stella Ortiz. El texto de la sentencia puede consultarse en: https://www.corteconstitucional.gov.co/relatoria/2021/C-032-21.htm

[34] D.1377/13, art. 26: Los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este decreto, en una manera que sea proporcional a lo siguiente: 1. La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente; 2. La naturaleza de los datos personales objeto del tratamiento; 3. El tipo de Tratamiento; 4. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares. En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, quienes

Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012". Así, resulta imposible ignorar la forma en que el Responsable del Tratamiento debe probar poner en funcionamiento medidas adecuadas, útiles y eficaces para cumplir la regulación. Es decir, el Responsable no puede utilizar cualquier tipo de políticas o herramientas para dicho efecto, sino solo aquellas que tengan como propósito lograr que los postulados legales sean realidades verificables, y no solo se limiten a creaciones teóricas e intelectuales.

Con el propósito de dar orientaciones sobre la materia, la Superintendencia de Industria y Comercio expidió el 28 de mayo de 2015 la *"Guía para implementación del principio de responsabilidad demostrada[35] (accountability)*"[36]. El término "***accountability***"[11], a pesar de tener diferentes significados, ha sido entendido en el campo de la protección de Datos como el modo en que una organización debe cumplir (en la práctica) las regulaciones sobre el tema, y la manera en que debe demostrar que lo puesto en práctica es útil, pertinente y eficiente. Conforme con este análisis, las recomendaciones que trae la guía a los obligados a cumplir la Ley Estatutaria 1581 de 2012, son:

(a) Diseñar y activar un programa integral de gestión de datos [sic] (en adelante PIGDP). Esto, exige compromisos y acciones concretas de los directivos de la organización. Igualmente requiere la implementación de controles de diversa naturaleza;
(b) Desarrollar un plan de revisión, supervisión, evaluación y control del PIGDP; y
(c) Demostrar el debido cumplimiento de la regulación sobre Tratamiento de Datos personales.

El Principio de Responsabilidad Demostrada –*accountability*- demanda implementar acciones de diversa naturaleza para garantizar el correcto cumplimiento de los deberes que imponen las regulaciones sobre Tratamiento de Datos Personales. El mismo, exige que los Responsables del Tratamiento adopten medidas apropiadas, efectivas y verificables que le permitan evidenciar la observancia de las normas sobre la materia. Dichas acciones o medidas deben ser objeto de revisión y evaluación permanente para medir su nivel de eficacia y el grado de protección de los Datos personales.

El Principio de Responsabilidad Demostrada precisa menos retórica y más acción en el cumplimiento de los deberes que imponen las regulaciones sobre Tratamiento de Datos personales. Requiere apremiar acciones concretas por parte de las organizaciones para garantizar el debido Tratamiento de los Datos Personales. El éxito del mismo, dependerá del compromiso real de todos los miembros de una organización. Especialmente, de los directivos de las organizaciones, pues, sin su apoyo sincero y decidido, cualquier esfuerzo será insuficiente para diseñar; llevar a cabo; revisar; actualizar y/o evaluar, los programas de gestión de Datos.

Adicionalmente, el reto de las organizaciones frente al Principio de Responsabilidad Demostrada va mucho más allá de la mera expedición de documentos o redacción de políticas. Como se ha manifestado, exige que se demuestre el cumplimiento real y efectivo en la práctica de sus funciones. En este sentido, desde el año 2006 la Red Iberoamericana de Protección de Datos (RIPD) ha puesto de presente que, "*la autorregulación sólo* [sic] *redundará en beneficio real de las personas en la medida que sea bien concebida, aplicada y cuente con mecanismos que garanticen su cumplimiento de manera que* ***no se constituyan en meras declaraciones***

---

efectúen el Tratamiento de los datos personales deberán suministrar a esta evidencia sobre la implementación efectiva de las medidas de seguridad apropiadas.

[35] El texto de la guía puede consultarse en: http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

[36] *El término inglés accountability puede ser traducido por rendición de cuentas. Esta voz inglesa, que, en su uso cotidiano, significa 'responsabilidad', ha comenzado a emplearse en política y en el mundo empresarial para hacer referencia a un concepto más amplio relacionado con un mayor compromiso de los Gobiernos y empresas con la transparencia de sus acciones y decisiones (...) el término accountability puede ser traducido por sistema o política de rendición de cuentas o, simplemente, por rendición de cuentas (...)"* Recuperado de https://www.fundeu.es/recomendacion/rendicionde-cuentas-y-norendimientomejor-que-accountability-1470/ el 22 de abril de 2019.

simbólicas de buenas intenciones sin que produzcan efectos concretos en la persona cuyos derechos y libertades pueden ser lesionados o amenazados por el tratamiento [sic] ***indebido de sus datos*** [sic] ***personales"***[37].(Destacamos).

El Principio de Responsabilidad Demostrada busca que los mandatos constitucionales y legales sobre Tratamiento de Datos personales sean una realidad verificable y redunden en beneficio de la protección de los derechos de las personas. Por eso, es crucial que los administradores de las organizaciones sean proactivos respecto del Tratamiento de la información. De manera que, por iniciativa propia, adopten medidas estratégicas, idóneas y suficientes, que permitan garantizar: i) los derechos de los Titulares de los Datos personales y ii) una gestión respetuosa de los derechos humanos.

Para el efecto, el principio de Responsabilidad Demostrada demanda del Responsable del tratamiento el deber de cumplir con las obligaciones impuestas por el Régimen de Protección de Datos y garantizar el debido Tratamiento de los datos personales. Lo anterior se debe a que, el propósito de las organizaciones que son Responsables o Encargados del Tratamiento es más allá de la expedición o redacción de políticas para el supuesto cumplimiento de la normativa vigente; por lo que se busca que lo administradores de las organizaciones sea proactivos respecto al Tratamiento de la información de manera que por iniciativa propia adopten las medidas estratégicas capaces, entre otras, la seguridad en el Tratamiento de la información según su naturaleza.

Para la consecución de lo expuesto, es necesario que las organizaciones establezcan un "Sistema de Administración de Riesgos"[38] asociados al Tratamiento de datos personales que les permita identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan indicar la debida administración del riesgo a que están expuestos los datos personales.[39]

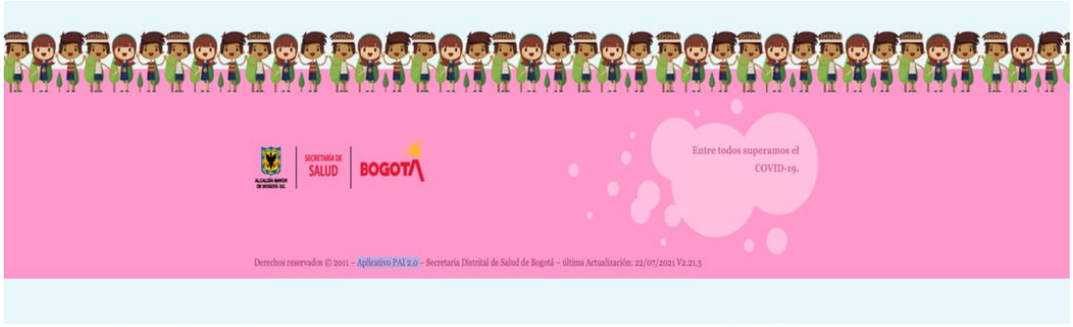
En el caso en concreto, se evidenció que: (i) el aplicativo PAI 2.0 carece de mención alguna a una PTI específica o general creada por parte de la Alcaldía Mayoy de Bogotá o la Secretaría de Salud y el Fondo Financiero de Salud; (ii) la PTI general de la Secretaría de Salud y el Fondo Financiero de Salud , en especial el contenido de la sección 5 sobre finalidades, resulta muy amplias para el Tratamiento de información, pues aun cuando se incorporó la mención de que el aplicativo PAI realiza la recolección de datos sensibles, no resulta suficiente en cuanto no contempla lo relacionado las condiciones especiales requeridas por el Régimen de Protección de Datos para el Tratamiento de datos sensibles, y; (iii) la sección 7 sobre la asignación del Responsable resulta ilegal considerando que asigna la calidad de Responsable del Tratamiento a una Entidad sin personería jurídica. Lo anterior no se ajusta a los preceptos establecidos por el Régimen de Protección de Datos, pues estos demandan que tal calidad sólo la puedan tener personas naturales y/o jurídicas, públicas o privadas.

---

[37] Cfr. Red Iberoamericana de Protección de Datos. Grupo de trabajo temporal sobre autorregulación y protección de datos personales. Mayo de 5 de 2006. En aquel entonces, la RIPD expidió un documento sobre autorregulación y protección de datos personales que guarda cercana relación con "accountability" en la medida que la materialización del mismo depende, en gran parte, de lo que interna mente realicen las organizaciones y definan en sus políticas o regulaciones internas.

[38] La Red Iberoamericana de Protección de Datos (RIPD) ha señalado que la autorregulación solo redundadará un beneficio real de las personas en la medida que sea bien concebida, aplicable y cunete con mecanismos que garanticen su cumplimiento de manera que no parezcan meras declaraciones simbólicas de buenas intenciones sin que se produzcan efectos concretos en las personos cuyos derechos y libertades pueden ser lesionados o amenazados por el tratamiento indebido de sus datos personales.

[39] Superintedencia de Industria y Comercio, "Guia de Implementación del Principio de Responsabilidad Demostrada – "Accountability", p. 16 – 18 (Superintendencia de Industria y Comercio, 2015).



Fuente:Parte inferior del aplicativo donde se evidencia que carece PTI o AP específica.

5. TRATAMIENTO Y FINALIDADES DE LA INFORMACIÓN O DATOS PERSONALES

La recolección y tratamiento de los datos personales tiene las siguientes finalidades:

a) Desarrollar la misión institucional, cumpliendo los objetivos y funciones según Resolución No. 1139 de fecha 28 de junio de 2017 y las normas que le fijen funciones a la Secretaria Distrital de Salud / Fondo Financiero Distrital en Salud.

b) Cumplir la normatividad vigente.

c) Gestionar y administrar los trámites y servicios ofrecidos por la Secretaria Distrital de Salud/ Fondo Financiero Distrital en Salud

d) Enviar por medios tradicionales y electrónicos información relacionada con la Secretaria Distrital de Salud/ Fondo Financiero Distrital en Salud, sus programas, actividades, noticias y demás trámites y servicios ofrecidos por la entidad.

e) Tramitar servicios de Gobierno Digital.

El tratamiento de la información que La Secretaría Distrital de Salud realiza es la de recolectar, almacenar y custodiar, información sensible a través de sus sistemas de información, los cuales proporcionan un servicio al ciudadano y que por tanto es información que no se encuentra de acceso al público, entre ellas tenemos el aplicativo PAI (Programa Ampliado de Inmunizaciones), comprobador de derechos (consulta de puntajes del sisben), Cuídate sé feliz (información útil para la salud de los ciudadanos), entre otros.

Fuente:Seccion 5 de la PTI general de la Secretaría de Salud y Fondo Financiero de Salud donde se evidencia la ausencia de lenguaje específico y apropiado para el tratamiento de información sensible

7. ENCARGADOS DE LA PROTECCIÓN Y TRATAMIENTO DE DATOS PERSONALES

1. Encargados de la protección de datos personales Secretaria Distrital de Salud/ Fondo Financiero Distrital en Salud.

2. Responsable del tratamiento Secretaria Distrital de Salud/ Fondo Financiero Distrital en Salud.

Punto de atención presencial: Carrera 32 No. 12- 81, Bogotá, código postal 0571.
Horario de atención: lunes a viernes de 7:00 a.m. a 4:30 p.m. en jornada continua.
Solicitudes, sugerencias, quejas o reclamos: contactenos@saludcapital.gov.co
PBX: (57-1) 3649090- 3649666.

Fuente:Seccion 7 de la PTI general de la Secretaría de Salud y Fondo Financiero de Salud donde se evidencia la designación como responsable a entidad sin personería jurídica.

En vista de lo anterior, se advierte que: (i) es posible que en la práctica la Alcaldía Mayor de Bogotá, para efectos de la Secretaría de Salud y Fondo Financiero de Salud, no haya implementado una estructura administrativa proporcional y adecuada a la magnitud del Distrito y los datos que este pueda recolectar, tratar, y resguardar, y; (ii) Los mecanismos internos para poner en práctica las PTI, incluyendo las herramientas de implementación de seguridad, son

insuficientes e ineficientes, puesto que con ingeniería inversa se logró el acceso a los datos de terceros ignorando los mecanismos de seguridad establecidos para el efecto; lo cual lleva a indicar que el sistema de administración de riesgos del Distrito no previene la materialización de vulneraciones a los principios para el debido Tratamiento de los datos personales, como la seguridad y el acceso y la circulación restringida de la información, contrariando así el principio de Responsabilidad Demostrada[40].

Por tanto, se recomienda a la Alcaldía Mayor de Bogotá, en su calidad de Responsable del Tratamiento, que adopte, entre otras, las siguientes medidas de Responsabilidad Demostrada :

(a) Desarrollar una Política de Protección de Datos específica, o adecuar la actual, con el fin de que se contemple las medidas de necesarias para la protección de datos sensibles de salud de los titulares;

(b) Designar de forma expresa a la Alcaldía Mayor de Bogotá D.C., como el Responsable del Tratamiento, y como área encargada a la Secretaría de Salud y Fondo de Financiero de Salud;

(c) Implementar de forma efectiva y comprobable un Sistema de Administración de Riesgos para efectos de los datos que el Distrito Administra y aplicable a las entidades del orden central.

(d) Incorporar medidas de Privacidad desde el Diseño y por Defecto en el diseño y desarrollo de aplicativos o herramientas tecnológicas o de cualquier índole a través de las que se realice Tratamiento de datos personales. Especial énfasis debe realizarse en que dichas medidas garanticen, entre otros, los principios de seguridad, confidencialidad y acceso y circulación restringida de los datos personales de los ciudadanos.

CONCLUSIONES:

El artículo 21 de la Ley Estatutaria 1581 de 2012 asignó a esta entidad la función de "*ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data*" así como "*impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disposiciones previstas en la presente ley*".

Dado lo anterior, se emitirán órdenes a la **ALCALDÍA MAYOR DE BOGOTÁ** para que garantice el debido Tratamiento de los datos personales de los ciudadanos de conformidad con lo señalado en la citada ley y teniendo en cuenta lo siguiente:

(a) La Alcaldía Mayor de Bogotá D.C., por intermedio de la Secretaría de Salud y el Fondo Financiero de Salud, habilitó el aplicativo PAI 2.0. en https://appb.saludcapital.gov.co/pai/publico/busqueda.aspx para que los ciudadanos pudieran consultar su respectivo certificado digital de vacunación contra el virus pandémico Coronavirus 2019 ("COVID-19)

(b) El aplicativo PAI 2.0 carece de medidas de seguridad, confidencialidad y de acceso y circulación restringida que sean técnicas, eficaces, necesarias y demostrables para evitar

[40] Con respecto a la aplicación práctica de la responsabilidad demostrada es necesario tener en cuenta lo resuelto por este Despacho en *In re* Facebook, R. 1321/19, Exp. 18 - 233402 (SIC, 2018), en la cual se estableció que el Responsable y/o Encargado del tratamiento tienen el deber constitucional de administrar correctamente y de proteger los archivos y bases de datos que contengan información personal y socialmente relevante, y para el efecto debe implementar las medidas apropiadas, útiles y eficaces para cumplir con la regulación, lo que siginifca que el Responsable no puede utilizar cualquier tipo de Política o herramienta para dicho efecto sino aquellas que sirvan para el cumplimiento de los postulados legales y que no sean meras elubricaciones teóricas sino realidades verificables.

el acceso no autorizado de terceros. Estas falencias fueron especialmente evidentes en la función de "Consultas" de dicho aplicativo, en tanto solo se requiere del número de ID, asignado a cada titular vacunado, introduciéndolo dentro del URL fijo para acceder a los datos de terceros sin sujetarse nuevamente a las medidas de seguridad -captcha-. Dicha función fue suspendida por parte de la ALCALDÍA MAYOR DE BOGOTÁ, según comunicado de prensa del 13 de agosto de 2021.

(c) El mencionado aplicativo permitió que cualquier persona accediera a datos personales sensibles de otras personas.

(d) El aplicativo PAI 2.0, que actualmente sigue operando pero sin la función de "Consultas", carece de referenciación al Aviso de Privacidad y Política Tratamiento de Información con el lenguaje exigido por el Régimen de Protección de Datos para el Tratamiento de información sensible

(e) La ALCALDÍA MAYOR DE BOGOTÁ no ha implementado un Sistema de Administración de Riesgos robusto en cumplimiento del Principio de Responsabilidad Demostrada.

(f) La ALCALDÍA MAYOR DE BOGOTÁ debe asegurar que sus desarrollos tecnológicos cumplan debidamente la normativa en materia de Tratamiento de protección de datos personales. Con el fin de lograr este objetivo, la privacidad y el debido Tratamiento de datos personales debe tomarse en cuenta desde el inicio del diseño de cualquier desarrollo tecnológico.

(g) La regulación sobre Tratamiento de Datos Personales debe aplicarse al margen de los procedimientos, metodologías o mecanismos que se utilicen para recolectar, usar o tratar ese tipo de información. Por ende, dicha regulación debe ser cumplida por la ALCALDÍA MAYOR DE BOGOTÁ o cualquier entidad pública o empresa que realice Tratamiento de datos mediante el uso de técnicas, herramientas como, entre otros, en internet, las App, la inteligencia artificial, la robótica, la computación en la nube, el internet de las cosas, etc.

El uso de esas innovaciones tecnológicas no hace desaparecer la protección de datos ni debe convertirse en un instrumento para disminuir el nivel de protección de los derechos de las personas que es exigido por la Ley Estatutaria 1581 de 2012.

En mérito de lo expuesto, esta Dirección

RESUELVE

ARTÍCULO PRIMERO. ORDENAR a la **ALCALDÍA MAYOR DE BOGOTÁ D.C.**, identificada con el NIT. 899.999.061-9, para que, como Responsable del Tratamiento, por intermedio de la SECRETARÍA DE SALUD Y EL FONDO FINANCIERO DE SALUD, como área Encargada, o quien haga sus veces, proceda a implementar mecanismos oportunos, útiles, necesarios, eficientes, eficaces y demostrables que fortalezcan las medidas de seguridad, confidencialidad, uso limitado, acceso y circulación restringida de los datos personales, en especial, los de naturaleza sensible que se encuentran en el aplicativo PAI 2.0, así como en cualquier otro desarrollo tecnológico o de otra índole que se pretenda implementar o que se esté implementando en el que se realice Tratamiento de Datos Personales. Especial énfasis deberá realizarse en el evento en que nuevamente se habilite la función de "Consulta" del aplicativo PAI 2.0.

Para lo anterior, se podrán tener en cuenta, entre otras, las recomendaciones realizadas en la parte considerativa del presente acto administrativo y, en particular, lo siguiente:

- **Antes de difundir al público o de poner a disposición de los usuarios** el aplicativo PAI 2.0 o cualquier otro desarrollo tecnológico o de otra índole, la ALCALDÍA MAYOR DE BOGOTÁ debe realizar pruebas para detectar eventuales fallas o errores con el objetivo de asegurar el cumplimiento de la regulación sobre Tratamiento de datos personales. Especialmente, debe garantizar que no se ocasionen vulneraciones a los derechos de las personas, y que las medidas de seguridad sean útiles para proteger la información y garantizar la confidencialidad, el acceso o la circulación restringida de los datos personales privados, semiprivados y sensibles

ARTÍCULO SEGUNDO. ORDENAR a la **ALCALDÍA MAYOR DE BOGOTÁ D.C.**, identificada con el NIT. 899.999.061-9, para que, como Responsable del Tratamiento, por intermedio de la SECRETARÍA DE SALUD Y EL FONDO FINANCIERO DE SALUD, como área Encargada, o quien haga sus veces, procedan a la implementación efectiva e inmediata del Principio de Responsabilidad Demostrada para efectos del aplicativo PAI 2.0, así como en cualquier otro desarrollo tecnológico o de otra índole que se pretenda implementar o que se esté implementando en el que se realice Tratamiento de Datos Personales. Para lo anterior, se podrán tener en cuenta, entre otras, las recomendaciones realizadas en la parte considerativa del presente acto administrativo.

ARTÍCULO TERCERO. La **ALCALDÍA MAYOR DE BOGOTÁ D.C.**, identificada con el NIT. 899.999.061-9, deberá cumplir lo ordenado en los artículos anteriores dentro de los dos (2) meses siguientes a la ejecutoria del presente acto administrativo.

PARÁGRAFO. Para demostrar el cumplimiento a que se refiere este artículo la **ALCALDÍA MAYOR DE BOGOTÁ** deberá remitir una certificación suscrita por la Alcaldesa Mayor de Bogotá D.C. mediante la cual acredite que se han implementado las medidas ordenadas y mencione las acciones que adoptaron para dar cumplimiento a las mismas.

ARTÍCULO CUARTO. ORDENAR a la **ALCALDÍA MAYOR DE BOGOTÁ D.C.**, identificada con el NIT. 899.999.061-9, que **SE ABSTENGA de poner en funcionamiento sistemas de información en internet u otros medios de divulgación y comunicación masiva** que contengan datos personales privados, semiprivados o sensibles **sin que previamente haya verificado que existen procesos, mecanismos, herramientas y controles técnicos o de cualquier otra naturaleza que sean pertinentes, efectivos y útiles para brindar un conocimiento o acceso restringido sólo a los Titulares de los datos personales o terceros autorizados conforme a lo señalado en la Ley Estatutaria 1581 de 2012**.

Para lo anterior se debe tener en cuenta lo siguiente:

- **Previo a difundir al público o de poner en funcionamiento sistemas de información o bases de datos en internet u otros medios de divulgación y comunicación masiva** que contengan datos personales privados, semiprivados o sensibles, la **ALCALDÍA MAYOR DE BOGOTÁ** deberá realizar pruebas para detectar eventuales fallas o errores con el objetivo de asegurar el cumplimiento de la regulación sobre Tratamiento de datos personales. Especialmente, debe garantizar que no se ocasionen vulneraciones a los derechos de las personas, y que las medidas de seguridad sean útiles para proteger la información y garantizar la confidencialidad, el acceso limitado y la circulación restringida de los mencionados datos personales.

- Antes de la implementación de desarrollos tecnológicos o de cualquier otra naturaleza que implican recolección, uso o tratamiento de datos personales la **ALCALDÍA MAYOR DE BOGOTÁ** deberá efectuar un estudio que incluya, como mínimo, lo siguiente: a) Una descripción detallada de las operaciones de tratamiento de datos personales que involucra el desarrollo tecnológico; b) Una evaluación de los riesgos específicos para los derechos y libertades de los titulares de los datos personales, y c) Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad, diseño de software, tecnologías y mecanismos que garanticen el debido tratamiento de los datos personales.

- Con anterioridad a la recolección o uso de los datos personales y durante todo el tiempo que trate esa información, la **ALCALDÍA MAYOR DE BOGOTÁ** deberá adoptar medidas preventivas de diversa naturaleza (tecnológica, organizacional, humana, procedimental, entre otras) con el objeto de evitar indebidos tratamientos de datos personales o fallas de seguridad que permitan, entre otras: (i) accesos indebidos o no autorizados a la información; (ii) manipulación o destrucción de la información; (iii) usos indebidos o no autorización de la información y (iv) circulación o suministro de datos personales a personas no autorizadas.

ARTÍCULO QUINTO. Notificar el contenido de la presente resolución a la **ALCALDÍA MAYOR DE BOGOTÁ D.C.**, identificada con el NIT. 899.999.061-9, informándole que contra el presente acto administrativo procede recurso de reposición ante la Directora de Investigación de Protección de Datos Personales (E) y de apelación ante el Superintendente Delegado para la Protección de Datos Personales, dentro de los DIEZ (10) días siguientes a la diligencia de notificación.

NOTIFÍQUESE Y CÚMPLASE
Dada en Bogotá D. C., octubre 5 de 2021

La Directora de Investigación de Protección de Datos Personales (E),

MARIA EUGENIA GUTIERREZ DARWICH

Firmado digitalmente por MARIA EUGENIA GUTIERREZ DARWICH
Fecha: 2021.10.05 09:24:51 -05'00'

MARÍA EUGENIA GUTIÉRREZ DARWICH

Proyectó: JATS
Revisó: MEGD
Aprobó: MEGD

Por la cual se imparte una orden administrativa

VERSIÓN
ÚNICA

NOTIFICACIÓN:

Entidad:	**ALCALDIA MAYOR DE BOGOTÁ D.C.**
NIT.:	899.999.061-9
Representante Legal:	CLAUDIA NAYIBE LÓPEZ HERNÁNDEZ
Identificación	C.C. 51.992.648
Dirección:	Carrera 8 número 10 – 65
Ciudad:	Bogotá D.C. – Colombia
Correo electrónico:	notificacionesjudiciales@secretariajuridica.gov.co