



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

RESOLUCIÓN NÚMERO 45002 DE 2020

(05 AGOSTO 2020)

Por la cual se imparte una orden administrativa

Radicación 20-153629

VERSIÓN ÚNICA

EL DIRECTOR DE INVESTIGACIÓN DE PROTECCIÓN DE
DATOS PERSONALES

En ejercicio de sus facultades legales, en especial las conferidas por el artículo 19 y 21 de la Ley 1581 de 2018 y el artículo 17 del Decreto 4886 del 2011, y

CONSIDERANDO

PRIMERO: Que la Alcaldía Mayor del Distrito de Bogotá D.C., con el fin de tener control sobre la población de la ciudad en relación con los síntomas del virus COVID-19, puso en funcionamiento los aplicativos denominados “Bogotá Cuidadora” – localizado en la página web www.bogota.gov.co/bogota-cuidadora- y “GABO APP”; y en cuyos formularios se solicitan los datos personales que se relacionan a continuación:

- 1.1. El Sub-aplicativo denominado “Registro de movilidad Segura”, solicita: (i) tipo y número de identificación; (ii) nombres completos; (iii) localidad y dirección de residencia; (iv) correo electrónico; (v) y número de celular. Adicionalmente, se exhorta al ciudadano, dentro del cuestionario de “Movilidad Inteligente”, a responder los siguientes cuestionamientos: (i) ¿Hacia qué localidad te vas a dirigir a realizar la actividad autorizada?; (ii) ¿En qué medio de transporte te desplazarás?; (iii) ¿A que hora saldrás a cumplir con la actividad seleccionada?, y; (iv) ¿Cuál es la hora de salida hacia tu hogar desde el sitio donde vas a realizar la actividad autorizada?. A lo cual se suma la siguiente serie de preguntas destinadas a individualizar que tipo de actividad van a realizar los Titulares. Finalmente, se indica que, para enviar el formulario e inscribirse en el sub-aplicativo, es necesario aceptar “(...) la Política de Privacidad y Tratamiento de Datos Personales, el “Manual de Políticas y Procedimientos para el Tratamiento de Datos Personales” de la Secretaría General de la Alcaldía Mayor de Bogotá, D. C. y la Política de Privacidad de GABO APP.”
- 1.2. En el sub-aplicativo denominado “Necesito Apoyo”, se solicita: (i) tipo y número de identificación; (ii) nombres completos; (iii) localidad y dirección de residencia; (iv) estrato; (v) fecha de nacimiento; (vi) correo electrónico; (vii) y número de celular. A lo cual se le suma el cuestionario de solicitud de ayudas especificando el tipo de ayuda a solicitar. Finalmente, se indica al inicio del registro que:

“Registra tus datos para poder acceder a los apoyos dispuestos por la Alcaldía en el marco de la emergencia COVID -19. Se informa que los datos suministrados serán tratados para la identificación de población que requiere ayuda a raíz de la epidemia del covid-19. Los datos suministrados serán tratados de conformidad con lo establecido en la Resolución 777 de 2019 por medio de la cual se adopta la Política de Privacidad y Tratamiento de Datos Personales y el “Manual de Políticas y Procedimientos para el Tratamiento de Datos Personales” de la Secretaría General de la Alcaldía Mayor de Bogotá, D. C. Para mayor información consulte la Política de Privacidad de GABO APP”

Finalmente, se indica al inicio del registro que: *“Al enviar el formulario de solicitud de apoyo estás aceptando la Política de Privacidad y Tratamiento de Datos Personales, el “Manual de Políticas y Procedimientos para el Tratamiento de Datos Personales” de la Secretaría General de la Alcaldía Mayor de Bogotá, D. C. y la Política de Privacidad de GABO APP.*

- 1.3. En el sub-aplicativo denominado “Reportar Estado de Salud” se solicita: (i) tipo y número de identificación; (ii) nombres completos; (iii) dirección de residencia y teléfono; (iv) correo electrónico; (vii) EPS, Y; (viii) fecha de nacimiento. El Titular debe responder también los

Por la cual se imparte una orden administrativa

VERSIÓN ÚNICA

siguientes cuestionamientos: (i) ¿Tiene alguno de los siguientes síntomas?, lo cual se responde con si o no; (ii) Fiebre cuantificada mayor o igual a 38°, Tos, dificultad para respirar, dolor de garganta (Odinofagia), dolor de cabeza persistente, fatiga/decaimiento o debilidad, diarrea o vómito, y otros (trastornos neurológicos).

1.4. Para la recolección y tratamiento de los datos anteriormente mencionados, la Alcaldía Mayor dispuso para las Plataformas el documento denominado “Política de privacidad de GABO App” en la cual se determinan como finalidades de las Plataformas, la siguientes:

1. *“Facilitar la atención y el registro de necesidades de los ciudadanos durante el estado de calamidad pública declarado en el Distrito Capital; minimizar los riesgos de contagio y propagación de la epidemia del covid-19, contar con información precisa que permita la identificación de personas contagiadas y propender por una reactivación económica segura, así como la identificación de población que requiere ayuda.*
2. *Optimizar la gestión de los trámites y servicios ofrecidos a la ciudadanía a través de la aplicación móvil GABO y SuperCADE Virtual.*
3. *Hacer el Registro de Movilidad Segura con el fin de dar cumplimiento a la obligación de identificación o acreditación de que trata el parágrafo 1o del artículo 3 del Decreto 749 de 2020, se aclara que el registro de movilidad nos es obligatorio, se debe hacer solo una vez y únicamente para registrar actividades económicas.*
4. *Obtener información de los ciudadanos para poder vincularlos a las distintas iniciativas y programas distritales;*
5. *Reporte de autocuidado frente al COVID-19 para la atención de la emergencia sanitaria.*
6. *Georreferenciación en tiempo real, que permitirá a la administración distrital, brindar atención e información eficaz y oportuna a los ciudadanos, durante el estado de calamidad pública declarado en el Distrito Capital y realizar seguimiento al cumplimiento de los lineamientos, medidas y controles generales adoptados por el Decreto 126 de 2020 para el manejo del riesgo derivado de la pandemia por Coronavirus COVID-19. Esta funcionalidad requerirá la autorización del usuario, quien podrá revocarla en cualquier momento.*
7. *Analítica de Datos que le permitirá a la administración distrital, la toma de decisiones estratégicas en atención a las diferentes necesidades ciudadanas que surjan a raíz de la emergencia COVID-19 y a la ciudadanía para obtener información de primera mano que le permita mejorar la toma de decisiones. “*

SEGUNDO: Que en virtud de lo anterior, esta Dirección, mediante los radicados 20-153629- -0-0 del 2 de junio de 2020 y 20-153629- -3-0 del 24 de junio de 2020, requirió a la Alcaldía Mayor de Bogotá D.C., para que respondiera los siguientes cuestionamientos:

1. *¿La recolección y tratamiento de los datos la realizan directamente la Alcaldía de Bogotá o se acude a los servicios de un tercero (Encargado de Tratamiento) para que se encargue de todos o algunos de los aspectos que involucra del tratamiento de datos personales? En caso que acudan a los servicios de un tercero, por favor adjuntar el contrato correspondiente para la prestación de dichos servicios.*
2. *¿Antes de diseñar la página web y aplicación, en lo relacionado con la recolección de datos, se realizó un estudio de impacto de privacidad (Privacy Impact Assessment - PIA por sus siglas en inglés)? En caso positivo, remitirnos dicho estudio.*
3. *¿Se realizó una evaluación de los riesgos específicos para los derechos y libertades de los Titulares de los datos personales? En caso positivo, anexar documento que acredite evidencia de ello.*
4. *¿Se desarrolló y puso en marcha un sistema de administración de riesgos asociados al tratamiento de datos personales que les permita “identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del*

Por la cual se imparte una orden administrativa

riesgo a que están expuestos los ciudadanos por o con ocasión del tratamiento de sus datos personales a través de la página web y aplicación? En caso positivo, anexas documento que acredite evidencia de ello.

5. ¿Qué medidas útiles, apropiadas, oportunas, efectivas y demostrables han adoptado para cumplir la regulación de tratamiento de datos personales respecto de la información que recolectan a través de la página web y la aplicación?
6. ¿Qué medidas tecnológicas; humanas; administrativas; físicas; contractuales y de cualquier otra índole han implementado para evitar:
 - a) Accesos indebidos o no autorizados a la información;
 - b) Manipulación de la información;
 - c) Destrucción de la información;
 - d) Usos indebidos o no autorización de la información?
 - e) Circulación o suministro de la información a personas no autorizadas.?
7. ¿Esas medidas de seguridad son objeto de revisión, evaluación y mejora permanente?
8. De conformidad con lo establecido en el artículo 11 del Decreto 1377 de 2013 (compilado en el Decreto 1074 de 2015), atendiendo las limitaciones temporales en el tratamiento de datos personales ¿tiene la Alcaldía de Bogotá establecido el procedimiento para la supresión de la información que sea recolectada en la citada página web y aplicación?
9. De conformidad con lo establecido en el artículo 4 del Decreto 1377 de 2013 (compilado en el Decreto 1074 de 2015) ¿qué procedimientos fueron establecidos para determinar que la información solicitada en el citado sitio web y aplicación, es **pertinente** y **adecuada** para la finalidad por la cual se está solicitando ese registro?
10. ¿Por qué razón cada uno de los datos recolectados es estrictamente necesario para cumplir la finalidad informada los ciudadanos?
11. Dentro de los procedimientos establecidos, ¿se tuvo en cuenta lo determinado en el artículo 6 de la Ley 1581 de 2012, en concordancia con el artículo 6 del Decreto 1377 de 2013, sobre el tratamiento de datos personales sensibles de los titulares?, en la medida que “ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles”.

TERCERO: Que mediante oficio radicado con el número 20-153629-6 de fecha 1 de julio de 2020, la Secretaria General de la Alcaldía Mayor de Bogotá en su calidad de Responsable del Tratamiento de conformidad con lo dispuesto en el Manual de Políticas y Procedimientos para el Tratamiento de Datos Personales, dio respuesta a los anteriores requerimientos, en los siguientes términos:

1. ¿La recolección y tratamiento de los datos la realizan directamente la Alcaldía de Bogotá o se acude a los servicios de un tercero (Encargado de Tratamiento) para que se encargue de todos o algunos de los aspectos que involucra del tratamiento de datos personales? En caso que acudan a los servicios de un tercero, por favor adjuntar el contrato correspondiente para la prestación de dichos servicios.

Respuesta: El proceso de recolección de datos y gestión de información es diferente en cada una de las funcionalidades de la plataforma web www.bogota.gov.co/bogota-cuidadora y de la aplicación móvil Gobierno Abierto de Bogotá -GABO-, anteriormente descritas, por lo tanto es importante aclarar que la información recolectada a través de las funcionalidades de Registro de Movilidad Segura y Necesito apoyo, es consolidada y tratada por el equipo de la Secretaria General.

Por su parte la información recolectada a través de la funcionalidad de Reporte Estado de Salud es gestionada directamente por la Secretaría Distrital de Salud donde se utilizan los datos a nivel espacial para encontrar patrones, para identificar casos sospechosos y para realizar el respectivo contacto para validación.

La infraestructura que la Secretaría General de la Alcaldía Mayor de Bogotá, D.C., ha dispuesto para la recolección y almacenamiento de los datos se encuentra soportada en los servicios de Microsoft que tiene contratados la entidad de conformidad con lo establecido en el Acuerdo Marco de Servicios Nube Pública No. CCE-578-2017 para la Secretaría General de la Alcaldía Mayor de Bogotá D.C., atendiendo a lo definido en el lineamiento LI.ST.04 de Acceso a servicios

Por la cual se imparte una orden administrativa

VERSIÓN ÚNICA

de la Nube del Marco de Referencia de Arquitectura de la Política de Gobierno Digital, y conforme a ello el proveedor Microsoft se ocupa de toda la infraestructura y software base para la operación de los formularios; garantizando la disponibilidad de la plataforma en un 99.7%, sin que este servicio involucre alguna gestión sobre los datos recolectados.

En ese orden de cosas, y atendiendo a lo establecido en la cláusula 15 del referido Acuerdo Marco de precio No. CCE-578-2017, Microsoft como proveedor de servicios tecnológicos de la Secretaría General da cumplimiento a la normativa colombiana en materia de seguridad, privacidad de la información y protección de datos personales.

Para tal efecto, los documentos de la orden de compra No. 45816 a través de la cual se adquirieron los productos y servicios Microsoft para dar continuidad a las aplicaciones, sitios y/o páginas web a través del anexo el Acuerdo Marco de Precios No. CCE-578-2017 para la Secretaría General de la Alcaldía Mayor de Bogotá D.C., pueden ser consultados siguiendo este enlace <https://colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/ordenes-compra/45816> o pueden ser consultados directamente en la siguiente carpeta que hemos dispuesto para facilitar el acceso a la documentación de soporta la respuesta al presente requerimiento, disponible en: <https://alcaldiabogota.sharepoint.com/:f/r/sites/CONSEJERIATIC/Documentos%20compartidos/GABO/bOGOT%c3%a1cUIDADORA/requerimientos%20sic?csf=1&web=1&e=An9p1S>.

Es importante mencionar como soportes adicionales, los siguientes documentos corporativos por que se rige Microsoft principalmente, lo cuales pueden ser consultados en línea:

a. La Declaración de Privacidad, disponible al público en general disponible en (<https://privacy.microsoft.com.es-mx/privacystatement>) que aplica de manera general a todos sus productos y servicios.

b. El Addendum de Protección de Datos de los Servicios Online de Microsoft. Disponibles al público en general (disponible en: <https://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=16059>) que es el documento contractual por medio del cual Microsoft establece sus obligaciones con respecto al procesamiento y la seguridad de los datos del cliente y datos personales relacionados con los servicios Online y los Servicios Profesionales. Dicho Addendum es vinculante para Microsoft en la prestación de todos sus servicios en línea. En el caso específico de nuestros Contratos Enterprise, en el encabezado de dichos contratos, se indica que el documento Términos de los Servicios en Línea, actualmente denominado Addendum de Protección de Datos de los Servicios Online de Microsoft, hace parte integral del Contrato Enterprise. Lo anterior implica que el Addendum de Protección de Datos de los Servicios Online de Microsoft es un documento de obligatoriedad contractual para Microsoft. En la página 5 de dicho documento, a la fecha se establece que: "Microsoft cumplirá todas las leyes y reglamentos aplicables a su prestación de los Servicios Online, incluyendo cualquier ley aplicable en materia de notificación de violaciones de la seguridad y Requisitos de Protección de Datos. Sin embargo, Microsoft no es responsable del cumplimiento de ninguna ley o reglamento aplicable al Cliente o a su sector que no sea aplicable con carácter general a los proveedores de servicios de tecnologías de la información. Microsoft no determina si los Datos del Cliente incluyen información sujeta a alguna ley o reglamento específico. Todos los Incidentes de Seguridad están sujetos a los términos sobre Notificación de Incidentes de Seguridad que se presentan más abajo"

2. ¿Antes de diseñar la página web y aplicación, en lo relacionado con la recolección de datos, se realizó un estudio de impacto de privacidad (Privacy Impact Assessment - PIA por sus siglas en inglés)? En caso positivo, remitimos dicho estudio.

Respuesta: Como se mencionó anteriormente los desarrollos de la plataforma web "Bogotá Cuidadora" y la aplicación móvil Gobierno Abierto de Bogotá- GABO surgen como respuesta a la emergencia sanitaria ocasionada por el COVID – 19, y con el propósito de servir de canal oficial para atender con agilidad y eficiencia las necesidades de los ciudadanos brindar información oportuna a la ciudadanía sobre la evolución de las medidas tomadas por el distrito, monitorear el impacto de la propagación del COVID-19 en Bogotá, fortalecer el acompañamiento a las comunidades vulnerables de la ciudad y contribuir a la reactivación económica gradual y a la movilidad segura en todo el territorio de la ciudad.

En ese sentido, teniendo en cuenta los requerimientos de la Ley de Protección de Datos y de conformidad con lo establecido en la Resolución 777 de 2019 por medio de la cual se adoptó la Política de Privacidad y Tratamiento de Datos Personales y el "Manual de Políticas y Procedimientos para el Tratamiento de Datos Personales" de la Secretaría General de la Alcaldía

Por la cual se imparte una orden administrativa

VERSIÓN ÚNICA

Mayor de Bogotá, D.C., y atendiendo los lineamientos de la Guía para implementación del principio de responsabilidad demostrada (Accountability) se están implementando controles para gestionar los riesgos asociados al Tratamiento de Datos Personales y minimizar los datos que se solicitan a los usuarios de la aplicación.

Adicionalmente, teniendo como referente las buenas prácticas internacionales, estamos trabajando en la elaboración de una evaluación de Impacto de Privacidad, para ello, siguiendo las recomendaciones dadas por el CSIRT de Gobierno nos estamos guiando por los lineamientos dados por la Autoridad Española de Protección de Datos Personales disponibles en la Guía Práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas RGPD.

3. ¿Se realizó una evaluación de los riesgos específicos para los derechos y libertades de los Titulares de los datos personales? En caso positivo, anexar documento que acredite evidencia de ello.

Respuesta: De acuerdo con la respuesta dada en el punto anterior, y de conformidad con lo establecido en la Resolución 777 de 2019 por medio de la cual se adoptó la Política de Privacidad y Tratamiento de Datos Personales y el “Manual de Políticas y Procedimientos para el Tratamiento de Datos Personales” de la Secretaría General de la Alcaldía Mayor de Bogotá D.C., para la creación y definición de los campos dispuestos en los formularios disponibles en la plataforma web “Bogotá Cuidadora” y la aplicación móvil Gobierno Abierto de Bogotá- GABO, se usaron una serie de preguntas detonantes para analizar la gestión de los datos a recolectare de manera tal que se priorizará la protección de los datos personales de los usuarios, procurando el máximo de satisfacción de las finalidades descritas.

Conforme a lo anterior frente al cumplimiento de la normativa colombiana en materia de protección de datos personales, se verificó que la política de privacidad y seguridad de la información estuviese publicada, y contemplará los mecanismos mínimos para asegurar la integridad, disponibilidad, y la confidencialidad de la información.

Adicionalmente frente a los campos definidos en los formularios se validó que:

- Se exijan únicamente los datos requeridos y necesarios para cumplir con las finalidades descritas en la plataforma web “Bogotá Cuidadora” y la aplicación móvil Gobierno Abierto de Bogotá- GABO
- No se recolecten datos sensibles o de menores de edad.
- No e solicite o registre información confidencial o sensible si no es necesaria.
- Se informe de forma clara, directa y concisa las finalidades del tratamiento, y se explique que el suministro de esta información es voluntario y de ninguna informa condicione su entrega para acceder a un servicio.
- Se informe de forma clara los derechos de los usuarios, incluido el derecho a solicitar la supresión de datos personales.

Producto de esta verificación se elaboraron los correspondientes avisos de privacidad tanto para la plataforma web “Bogotá Cuidadora”, como para la aplicación móvil Gobierno Abierto de Bogotá- GABO y se elaboró un aviso específico para la funcionalidad de Registro de Movilidad Segura. Adicionalmente se validaron y minimizaron los campos de los formularios garantizando adicionalmente la experiencia de usuario de las funcionalidades dispuestas.

4. ¿Se desarrolló y puso en marcha un sistema de administración de riesgos asociados al tratamiento de datos personales que les permita “identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos los ciudadanos por o con ocasión del tratamiento de sus datos personales a través de la página web y aplicación? En caso positivo, anexar documento que acredite evidencia de ello.

Respuesta: La Secretaría General de la Alcaldía Mayor de Bogotá cuenta con procedimientos establecidos para realizar la gestión de riesgos atendiendo a lo definido tanto el Modelo de gestión de riesgos de seguridad Digital propuesto por MINTIC, como en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP. En ese sentido se toma como punto de referencia la guía para el inventario, clasificación, etiquetado de información, protección de datos personales y análisis de riesgos de los activos de información (4204000-GS-004) a su vez el procedimiento de activos de información (2213200-PR-187)¹.

¹ Documentos que pueden ser consultados directamente en la carpeta que hemos dispuesto para facilitar el acceso a la documentos de soporta la respuesta al presente requerimiento:

Por la cual se imparte una orden administrativa

VERSIÓN ÚNICA

Conforme a lo anterior, la gestión de riesgos de seguridad y privacidad de la información, se realiza a partir de la correcta identificación de los activos de información, estableciendo conforme a ellos los factores de riesgo, vulnerabilidad, causa / amenaza, consecuencia / efecto, probabilidad antes del control, impacto antes del control, dimensión del riesgo inherente, tipificación del riesgo, descripción de la actividad que actúa como control, probabilidad de ocurrencia luego de aplicar control, dimensión del riesgo residual.

De igual manera se realiza el diagnóstico de seguridad de la información, con el fin de conocer el estado de los controles de la norma ISO 27001, obteniendo un plan de acción donde se incluyen los controles que se encontraron con desviaciones, en la actualidad se está trabajando con los responsables de cada control, con el fin de establecer las actividades, fechas y responsables a fin de minimizar la materialización de riesgos.

Por consiguiente, en la fase de diseño del tratamiento de información que contiene datos personales, se define el flujo de los datos personales, así como todos los elementos que intervendrán a lo largo del mismo. De igual modo, se estructuran las medidas de control y seguridad que se implementan para garantizar los derechos y libertades de los interesados con el objetivo de que un tratamiento nazca respetando los requerimientos de privacidad asociados al nivel de riesgo a la que está expuesto.

La gestión de riesgos que se realiza en la Secretaría General para la gestión de sus activos de información se divide en tres etapas así: La identificación, la evaluación y el tratamiento de los riesgos. En este punto debemos aclarar que los procedimientos puntuales están siendo actualizados teniendo en cuenta las buenas prácticas internacionales que se han elaborado con ocasión del tratamiento de datos para la pandemia de la COVID -19, y se están engranando como la estrategia para incorporar la privacidad, la seguridad y la ética desde el diseño y por defecto como principios rectores en el tratamiento de la información para la Alcaldía Mayor de Bogotá.

En ese orden de ideas se realiza una caracterización y priorización y se identifican las amenazas y vulnerabilidades categorizando los controles a implementar para garantizar el cumplimiento de los principios de seguridad de la información.

- **Confidencialidad:** Amenazado por el acceso ilegítimo a los datos, y el daño que puede causar que lo conociera tercero no autorizados (fuga de información, uso ilegítimo de datos, pérdida de dispositivos móviles, acceso por personal no autorizado), para su gestión se establecen controles de acceso por personal no autorizado), para su gestión se establecen controles de acceso, a alertas para prevenir el acceso o intercambio de información no autorizada.

- **Integridad:** Amenazada por la modificación no autorizada de los datos, y el posible perjuicio causado si la información es dañada (errores en los procesos de recopilación y captura de datos, modificación no autorizada de datos de forma intencionada, suplantación de identidad), para su gestión también se hace uso de controles de acceso y se incorpora adicionalmente un control de cifrado que obliga a que siempre se comparta información esta vaya siempre cifrada.

- **Disponibilidad:** Amenazada por la eliminación de los datos, o indisponibilidad de estos y no poder utilizarlos, (error o ataque intencionado que provoque el borrado pérdida de datos, desastres naturales, cortes en el suministro eléctrico o en los servicios de comunicación), para su gestión se realizan copias de seguridad periódicas, y se prueban los mecanismos de recuperación de datos.

5. ¿Qué medidas útiles, apropiadas, oportunas, efectivas y demostrables han adoptado para cumplir la regulación de tratamiento de datos personales respecto de la información que recolectan a través de la página web y la aplicación?

Respuesta: Como hemos mencionado, el tratamiento de los datos recolectados a través del portal web www.bogota.gov.co/bogota-cuidadora y de la aplicación GABO se rigen por lo establecido en la Política de Privacidad y Tratamiento de Datos Personales y en el Manual de Políticas y Procedimientos para el Tratamiento de Datos Personales adoptados por la Secretaría General de la Alcaldía Mayor de Bogotá, D.C., a través de la Resolución 777 de 2019.

Por la cual se imparte una orden administrativa

VERSIÓN ÚNICA

De acuerdo con lo anterior, y teniendo lo establecido tanto el Modelo de gestión de riesgos de seguridad Digital propuesto por MINTIC, como en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP, la Secretaría General ha implementado controles de privacidad y seguridad de la información para garantizar la autenticidad, integridad y disponibilidad de la información bajo su custodia. Conforme a lo anterior, dentro de las medidas adoptadas tenemos:

- Se tienen establecidos mecanismos para revisar periódicamente que los permisos concedidos son adecuados, haciendo énfasis en los usuarios cuyos accesos han sido eliminados o modificados, y se comprueba con la periodicidad establecida en función de la clasificación de la información, la correcta asignación de los permisos. (De acuerdo al procedimiento 2213200pr-185, guía 2211700-GS-038 y lineamientos 4204000-OT-048).
- Se verifica por un lado los permisos concedidos a cada perfil y por otro, los usuarios asignados a cada perfil. (De acuerdo a los Procedimientos 2213200PR-185, 2213200-PR-273)
- Se presta especial atención a los servicios accesibles desde el exterior, como el uso del correo electrónico corporativo desde fuera de la empresa o el acceso de usuarios a nuestra infraestructura a través de VPN (red privada virtual). (De acuerdo a los lineamientos 4204000-OT-048 y acuerdos de confidencialidad)
- No se limita al control de acceso lógico y por el contrario se incluye cuando es necesario, controles de acceso físico. (De acuerdo a los Procedimientos 2213200-pr-273 y guía 2211700-gs-037).
- Se propende por el uso de repositorios en los cuales se puede evidenciar el log de eventos de acceso y consulta los repositorios. (De acuerdo al Procedimiento 2213200-pr-272).
- Las copias de seguridad son la salvaguarda básica para proteger la información, por tanto, se realizan de manera periódica pruebas de comprobación con el fin de determinar su integridad y disponibilidad. (De acuerdo al Procedimiento 2213200-PR109 y lineamientos 4204000-ot-048)
- Se utilizan estrategias de cifrado de la información que consiste en ofuscar la información mediante técnicas de codificación, evitando que los datos sean legibles por cualquier persona que desconozca la clave de decodificación. (De acuerdo a los lineamientos 4204000-ot-048).
- Referente a la destrucción física de soportes y contenedores de información personal, para los menos robustos (CD/DVD, papel) estos se destruyen de manera manual y los contenedores como discos duros son sanitizados mediante prácticas de borrado seguro). De acuerdo a la guía 2211700-gs-044)
- Por último, como una medida que mitiga riesgos por el acceso no autorizado a información clasificada, se tiene la firma de contratos de confidencialidad o inclusión de este tipo de cláusulas en el contrato con terceros contratistas y demás funcionarios de la entidad.

Adicionalmente se debe considerar que tanto el portal web www.bogota.gov.co/bogota-cuidadora y como la aplicación GABO se encuentran soportadas por la infraestructura de TI dispuesta por la Secretaría General para la administración de las soluciones, la cual permite un escalamiento de forma automática a medida que los usuarios ingresan a registrarse y garantiza la seguridad y privacidad de la información que recolecta, siendo esta almacenada en sistema de información seguros gestionados por la Oficina Tecnologías de Información y las Comunicaciones de la Secretaría General, los cuales cuentan con un control de acceso, soportado en una definición de perfiles y roles, que permite validar y verificar los usuarios que pueden tener acceso a la información.

Así mismo, la aplicación móvil Gobierno Abierto de Bogotá (GABO) realiza su comunicación encriptada mediante https, el componente que recibe el tráfico entrante de la aplicación móvil es un servidor WAF de AZURE del TENANT productivo de los servicios en la nube contratados por la Secretaría General, este componente ofrece la configuración de llaves públicas y privadas para encriptar información.

De otra parte, en una segunda iteración, los formularios disponibles en plataforma www.bogota.gov.co/bogota-cuidadora se trasladaron a un desarrollo en PHP realizado por el equipo de la Secretaría General, el cual permite la validación en los campos de captura, ofreciendo mayor calidad en la información recopilada.

En ambos casos esto se hace bajo un HTTPS (HyperText Transfer Protocol Secure), protocolo que protege la integridad y la confidencialidad de los datos entre el ordenador en el que diligencian y el sitio web que los recibe.

6. ¿Qué medidas tecnológicas; humanas; administrativas; físicas; contractuales y de cualquier otra índole han implementado para evitar:

a) Accesos indebidos o no autorizados a la información;

Por la cual se imparte una orden administrativa

VERSIÓN ÚNICA

- b) Manipulación de la información;
- c) Destrucción de la información;
- d) Usos indebidos o no autorización de la información?
- e) Circulación o suministro de la información a personas no autorizadas.?

Respuesta: Como se mencionó en la respuesta al punto anterior, los datos personales se recolectan atendiendo a la Política de Privacidad y Tratamiento de Datos Personales y al Manual de Políticas y Procedimientos para el Tratamiento de Datos Personales adoptados por la Secretaría General de la Alcaldía Mayor de Bogotá D.C., a través de la Resolución 777 de 2019; y se almacenan en sistemas de información seguros gestionados por la Oficina TIC de la Secretaría General, a través de los cuales se implementa un control de acceso, soportado en una definición de perfiles y roles, que permite validar y verificar que usuarios pueden tener acceso a la información, con lo cual se asegura el cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información.

Adicionalmente se siguen los lineamientos de la estrategia de Seguridad y Privacidad de la Información para la Alcaldía de Bogotá (2016-2020) disponible en; <http://ticbogota.gov.co/seguridad>, la cual señala que el manejo de la información debe respetar los siguientes criterios:

- El uso y gestión de los datos debe incorporar y apropiar las guías del Modelo de Seguridad y Privacidad del Mintic mediante la implementación, monitoreo y evaluación de la estrategia de manera sencilla y metódica.
- Se debe dar cumplimiento a todos los requisitos legales, reglamentarios y contractuales con respecto al manejo de la información.
- Se deben implementar las acciones correctivas que permitan eliminar las causas de problemas al interior de la entidad Distrital en temas de seguridad digital con el uso de las guías metodológicas propuestas.
- Se deben implementar metodologías para el manejo de activos de información a nivel distrital lo que permitan identificar, valorar y gestionar los riesgos de seguridad digital.

Por último, debemos mencionar que, con ocasión de la mesa de trabajo convocada por el CSIRT de Gobierno, actualmente se está trabajando de la mano del ColCERT, para realizar una prueba de concepto de seguridad sobre el portal web www.bogota.gov.co/bogota-cuidadora y de la aplicación GABO, a fin de hacer inteligencia de ataques cibernéticos, de manera anticipada previendo la materialización de estos, con base en conocimientos desarrollados por ellos.

7. ¿Esas medidas de seguridad son objeto de revisión, evaluación y mejora permanente?

Respuesta: Si. Los sistemas de información y las medidas de seguridad aplicadas se revisan regularmente para garantizar el cumplimiento de los estándares de implementación de la seguridad anteriormente descritos. Así mismo, con relación a los procedimientos de análisis, desarrollo y mantenimiento de las aplicaciones, se realizan revisiones técnicas y si en algún caso, no se cumple un control establecido dentro de las políticas de seguridad durante la verificación, éstas se corrigen antes de su puesta en producción identificando las causas del incumplimiento.

De igual manera, en el ciclo anual junto con el proceso de mejora continua de la Secretaría General se realizan las evaluaciones y ejercicios de mejora continua tal como se describe en lineamientos para la implementación y sostenibilidad del sistema de gestión de seguridad de la información y el cronograma de revisiones dispuesto por parte de la Oficina de Tecnología de la Secretaría General los cuales pueden ser consultados en: <https://alcaldiabogota.sharepoint.com/:u:/sites/CONSEJERIA/TIC/Documentos%20compartidos/GABO/Bogot%C3%A1Cuidadora/REQUERIMIENTOS%20SIC/06.%20Plan%20de%20tratamiento.rar?csf=1&web=1&e=0yv9Ss>

Por último, teniendo en cuenta las recomendaciones que entregue el ColCERT, sobre el estudio de concepto realizado sobre el portal web www.bogota.gov.co/bogota-cuidadora y de la aplicación GABO se realizarán los ajustes y correcciones pertinentes para actualizar las medidas de seguridad de la Secretaría General.

8. De conformidad con lo establecido en el artículo 11 del Decreto 1377 de 2013 (compilado en el Decreto 1074 de 2015), atendiendo las limitaciones temporales en el tratamiento de datos personales ¿tiene la Alcaldía de Bogotá establecido el procedimiento para la supresión de la información que sea recolectada en la citada página web y aplicación?

Por la cual se imparte una orden administrativa

VERSIÓN ÚNICA

Respuesta: Los datos que se están recolectando son tratados únicamente para las funcionalidades descritas, por lo tanto una vez se supere esta coyuntura, y los efectos que han llevado a desplegar estas acciones, los mismos serán eliminados de forma segura, proceso que se hará siguiendo lo establecido en el procedimiento y/o guía interna de borrado seguro, el cual se ha definido conforme a las directrices de gestión documental y de conformidad con lo establecido en la Ley de Protección de Datos, así como en nuestra Política de Privacidad y Tratamiento de Datos Personales y nuestro Manual de Políticas y Procedimientos para el Tratamiento de Datos Personales, garantizando de manera eficiente la eliminación o destrucción de información, basados en métodos que permitan el borrado seguro de la información almacenada en las bases de datos, evitando el acceso a la información contenida en las mismas o su recuperación posterior.

No obstante, los informes derivados del análisis de los registros anonimizados podrán ser utilizados para la realización de estudios, modelos y en general para documentar el proceso de Bogotá ante la pandemia COVID 19 en los diferentes frentes que se adelantan.

De igual manera, la Secretaría General de la Alcaldía Mayor de Bogotá, como responsable del Tratamiento de los datos recolecta a través de la plataforma web “Bogotá Cuidadora”, como de la aplicación móvil GABO APP, con el fin garantizar los derechos del titular de los datos personales, y cumpliendo lo establecido en los artículos 14 y 15 de la Ley 1581 de 2012 y en el artículo 2.2.2.26.24. del Decreto Único Reglamentario del Sector Comercio, Industria y Turismo 1074 de 2015, ha dispuesto diferentes medios de atención de peticiones, consultas y reclamos sobre datos personales, para que el titular pueda ejercer sus derechos a conocer, actualizar, rectificar y suprimir sus datos personales contenidos en bases de datos y revocar la autorización que haya otorgado para el tratamiento de los mismos, los cuales se encuentran señalados en la Política de Privacidad y Tratamiento de Datos Personales y en el Manual de Políticas y Procedimientos para el Tratamiento de Datos Personales de entidad adoptados mediante la Resolución 777 de 2019; así

Atención de peticiones, consultas y reclamos de Datos Personales

La Oficina de Tecnología de Información y Comunicaciones - OTIC en coordinación con la dependencia que tiene a cargo el correspondiente sistema de información, son las responsables de dar trámite a las solicitudes de los titulares para hacer efectivos sus derechos relacionados con el tratamiento de datos personales.

La SECRETARÍA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ tiene dispuestos los siguientes canales para recibir y atender las peticiones, consultas y reclamos relacionados con el tratamiento de datos personales:

| | |
|---------------------------------------|---|
| Correo electrónico | Bogotá Te Escucha http://www.bogota.gov.co/sdgs |
| Página web | Bogotá Te Escucha http://www.bogota.gov.co/sdgs Secretaría General http://secretariageneral.gov.co/ |
| Teléfonos | Línea 195 |
| Punto de atención escrito | Ventanilla de radicación Manzana Liévano |
| Punto de atención verbal o presencial | SuperCADE CADE Punto de Información Manzana Liévano |

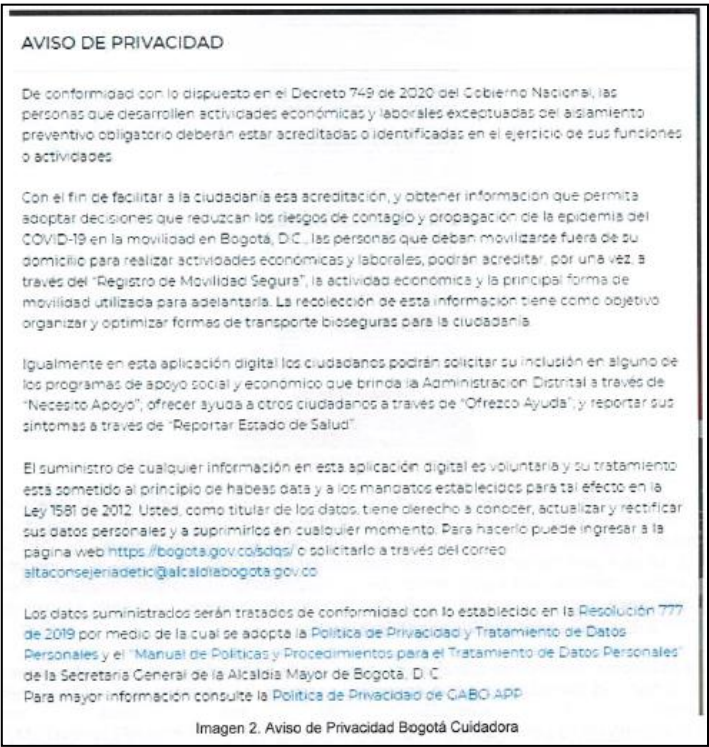
Estos son los únicos canales que la SECRETARÍA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ tiene habilitados para las consultas y reclamos por protección de datos personales, por lo tanto, el titular deberá tenerlos presente. El área encargada en ningún caso podrá dejar sin respuesta al titular, representante legal o causahabiente.

Imagen 1. Política de Privacidad y Tratamiento de Datos Personales

Aunado a ello, la Secretaría General de la Alcaldía Mayor de Bogotá , con el fin de garantizar que las personas puedan ejercer de manera plena su derecho de habeas data (conocer, actualizar, suprimir, rectificar sus datos personales) dispuso de manera adicional el correo electrónico altaconsejeriadetic@alcaldiabogota.gov.co; y el formulario de “Solicitud de Supresión de Datos”, los cuales en cumplimiento a lo establecido en el artículo 2.2.2.25.1.3 del Decreto Único Reglamentario del Sector Comercio, Industria y Turismo 1074 de 2015, fueron puestos en conocimiento de la ciudadanía a través del aviso de privacidad que aparece al acceder tanto a la plataforma web www.bogota.gov.co/bogota-cuidadora, como al registro de movilidad segura de la APP GABO, el cual informa al titular de los datos acerca de la existencia de las políticas de tratamiento de la información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales; como se observa a continuación:

Por la cual se imparte una orden administrativa

VERSIÓN ÚNICA

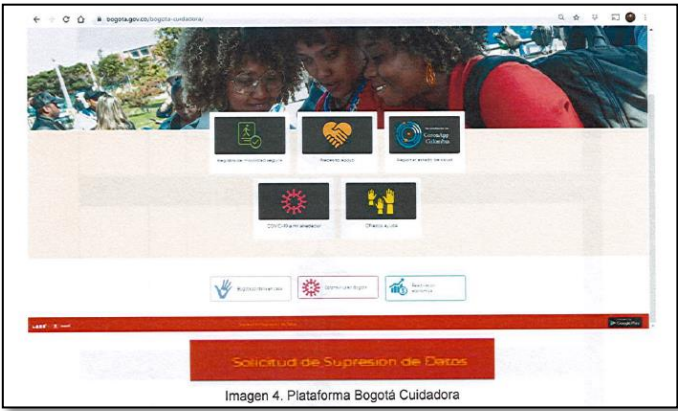


En estos avisos puntualmente se aclara al usuario que: “El suministro de cualquier información en esta aplicación digital es voluntaria y su tratamiento está sometido al principio de habeas data y a los mandatos establecidos para tal efecto en la Ley 1581 de 2012, en los siguientes términos: “Usted, como titular de los datos, tiene derecho a conocer, actualizar y rectificar sus datos personales y a suprimirlos en cualquier momento. Para hacerlo puede ingresar a la página web <https://bogota.gov.co/sdqs/> o solicitarlo a través del correo altaconsejeriadedetic@alcaldiabogota.gov.co”.

Demás, como se indicó en párrafos anteriores, en la parte inferior de la plataforma web (franja roja), se habilitó un espacio específico para que las personas que asó lo den soliciten la supresión de sus datos ver: <https://forms.office.com/Pages/ResponsePage.aspx?id=y6dR80r58E2WJ64DDM73xAWOsPtggIVEoXd0yQmVorxUQ1FRN0hZS1JMNUHwJNKTec2Q0hXV09ERC4u>

Por la cual se imparte una orden administrativa

VERSIÓN ÚNICA



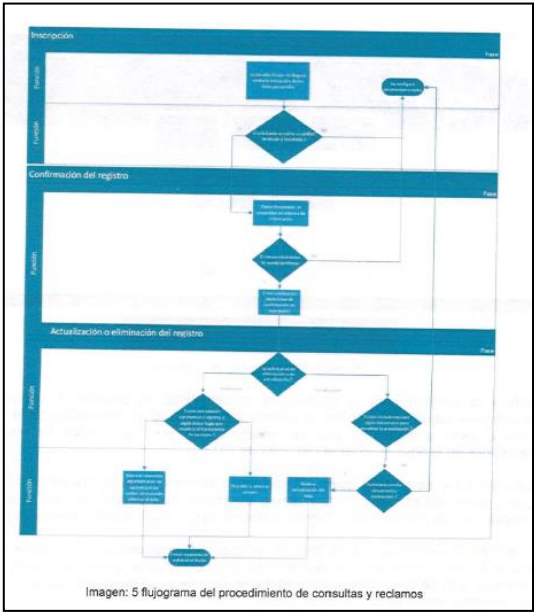
Recibida La solicitud para la gestión del requerimiento se procede a catalogar el requerimiento según sea consulta de información o solicitud de eliminación, teniendo en cuenta el canal a través del cual se recibió la petición y los tiempos de respuesta establecidos en el artículo 15 de la Ley 1581 de 2012.

Para validar que es el titular quien está actuando se tomarán en cuenta de los datos de ingreso como número de cédula y correo electrónico con el cual se hizo el registro, validando que los mismos correspondan a la solicitud de modificación.

En caso de no cumplir con los parámetros mínimos para gestionar la petición la Secretaría General deberá informar al titular dentro de los cinco días hábiles siguientes al recibo de la solicitud, a fin de que aporte la documentación faltante o cualquier otra aclaración que sea necesaria para la ejecución de la consulta.

En aquellos eventos en los cuales no se cuente con información suficientes para validar la legitimación en la causa para atender la solicitud o se considere que la petición no puede ser tramitada debido a que la Secretaría General de la Alcaldía Mayor de Bogotá no puede comprobar que la solicitud provenga directamente del titular de los datos personales, o porque exista normativa asociada que impida la supresión de los datos, la Secretaría General podrá integrar una mesa de trabajo entre la Oficina Asesora de Jurídica, Oficina de Tecnologías de la Información y las Comunicaciones, Alta Consejería Distrital de TIC, según corresponda, a efectos de contar con un concepto jurídico y técnico integral para dar efectiva respuesta al titular sobre el trámite y cumplimiento de su solicitud.

El siguiente flujograma detalla cómo se adelanta este proceso a nivel interno en la Secretaría General:



9. De conformidad con lo establecido en el artículo 4 del Decreto 1377 de 2013 (compilado en el Decreto 1074 de 2015) ¿qué procedimientos fueron establecidos para determinar que la

Por la cual se imparte una orden administrativa

información solicitada en el citado sitio web y aplicación, es **pertinente** y **adecuada** para la finalidad por la cual se está solicitando ese registro?

Respuesta: Como se mencionó anteriormente los desarrollos de la plataforma web “Bogotá Cuidadora” y la aplicación móvil Gobierno Abierto de Bogotá- GABO surgen como respuesta a la emergencia sanitaria ocasionada por el COVID -19, y con el propósito de servir de canal oficial para atender con agilidad y eficiencia las necesidades de los ciudadanos, brindar información oportuna a la ciudadanía sobre la evaluación de las medidas tomadas por el Distrito, monitorear el impacto de la propagación del COVID-19 en Bogotá, fortalecer el acompañamiento a las comunidades vulnerables de la ciudad y contribuir a la reactivación económica gradual y a la movilidad segura del Distrito.

Así, para la construcción de los formularios se verificó que se incluyeran únicamente los campos necesarios para cumplir con las finalidades que no se recolectarán datos sensibles o de menores de edad y que no se registre información confidencial o sensible si no es necesaria para la finalidad.

Conforme a lo anterior, en su primera versión, puesta en producción el 1 de junio de 2020, la plataforma web Bogotá Cuidadora y la aplicación Gobierno Abierto- GABO- se publicaron con las siguientes funcionalidades:

- a) **Necesito apoyo.** Permite a los ciudadanos solicitar ayudas que tiene el Distrito para atender la emergencia sanitaria generada por el COVID-19 (transferencias monetarias, bonos canjeables, alimentación escolar, etc.). Estas solicitudes son validadas y si se cumplen los requisitos estipuladas se brinda acceso a las mismas.
- b) **Reportar estado de salud.** Permite a los ciudadanos reportar su estado de salud. Así podemos hacer un mejor seguimiento de la enfermedad en Bogotá. A los ciudadanos les sirve para recibir atención más rápida en caso de síntomas agudos. La plataforma arroja información sobre los puntos de atención de salud más cercanos. Esta información la cruzamos con la que está disponible en CoronaAPP para combinar esfuerzos.
- c) **COVID-19 a mi alrededor:** Accede a los mapas y a los datos proporcionados por Saludata con el fin del que el ciudadano pueda saber cuántos contagiados hay por localidad y por edad, así como el porcentaje de ocupación de las Unidades de Cuidado Intensivo en Bogotá. Hay un mapa de calor que le ayuda a determinar cuáles de las zonas de la ciudad con mayor número de contagios confirmados.
- d) **Ofrezco Ayuda:** Accede a la Red de Cuidado Ciudadano y permite que los ciudadanos que quieran entregar apoyo lo hagan a través de este mecanismo.
- e) **SuperCADE Virtual:** (Solo disponible en Gabo APP) para facilitar a las personas permanecer en casa GABO APP incluye la APP Super CADE Virtual, que ha estado al servicio de los ciudadanos desde hace dos años y en donde se pueden hacer varios trámites desde el teléfono.
- f) **Registro de Movilidad Segura:** con el fin de dar cumplimiento a la obligación de identificación o acreditación de que trata el parágrafo 1 del artículo 3 del Decreto Nacional 749 de 2020, y con el objetivo de recolectar información estratégica para la toma de decisiones en movilidad y optimizar las formas de transporte en Bogotá.

10. ¿Por qué razón cada uno de los datos recolectados es estrictamente necesario para cumplir la finalidad informada los ciudadanos?

Respuesta: De conformidad con el ejercicio descrito en la respuesta al punto 6 se realizó un análisis de cada uno de los campos que se solicita, con los cuales se logra atender de manera exitosa las necesidades del ciudadano y/o tomar mejores decisiones para: garantizar una movilidad segura, hacer seguimiento epidemiológico y determinar cuáles son las necesidades más apremiantes de la ciudadanía.

Los datos que se piden se usan de la siguiente manera:

- **Tipo de Identificación.** Se utiliza para llevar el registro tanto en la aplicación como en el formulario web y para validar que el registro lo hagan mayores de edad.

Por la cual se imparte una orden administrativa

VERSIÓN ÚNICA

- *Número de Identificación. Se utiliza para el registro de la aplicación y para llevar el registro de la información en los formularios de la plataforma web.*
- *Fecha de Nacimiento. Se utiliza para el registro de la aplicación como en el formulario web. Esta dato se utiliza como mecanismo de validación para asegurar que el registro únicamente lo hagan mayores de edad.*
- *Nombre y Apellidos. Se utiliza para el registro de la aplicación y para llevar el registro de la información en los formularios de la plataforma web.*
- *Localidad de residencia. Se utiliza para conocer de forma referencial los puntos de inicio de los desplazamientos y para identificar los puntos de atención para los posibles apoyos a suministrar.*
- *Dirección de residencia. Se utiliza para conocer de forma concreta los puntos de inicio de los desplazamientos y para identificar los puntos de atención para los posibles apoyos a suministrar.*
- *Correo electrónico. Se utiliza para llevar el registro de la aplicación y como mecanismo de contacto con los usuarios.*
- *Número de celular: Se utiliza para llevar el registro de la aplicación y mecanismo de contacto con los usuarios.*

Imagen 6. Registro GABO

De igual forma el formulario web de Registro de Movilidad Segura solicita la información para realizar ejercicios de movilidad, consultando la localidad hacia la cual se va a dirigir la persona a realizar la actividad autorizada, en qué medio de transporte se hará el desplazamiento y en que franja horaria retornará de realizar su actividad económica y por último le pide selección de la principal razón por la cual se genera el desplazamiento, pidiéndole seleccionar una de las excepciones que se han establecido en la normatividad Nacional y Distrital para autorizar la movilidad, así:

Por la cual se imparte una orden administrativa

VERSIÓN ÚNICA

Reporte de movilidad segura
Reporte un cambio respecto a tu movilidad segura

La Alcaldía Mayor de Bogotá pone a disposición de la ciudadanía el presente Registro de Movilidad Segura con el fin de dar cumplimiento a la obligación de identificación y verificación de que todos los habitantes de Bogotá, en cumplimiento de la Ley 1612 de 2016, se identifiquen y verifiquen sus datos personales, laborales, comerciales y académicos, para garantizar la seguridad y el bienestar de la ciudad. Se informará a la ciudadanía sobre los beneficios de la movilidad segura y se brindará asistencia técnica y logística para facilitar el proceso de registro. Los datos suministrados serán tratados de conformidad con la legislación en la Resolución 007 de 2019 por medio de la cual se adopta el Plan de Privacidad y el Plan de Retención de Datos Personales y el Plan de Retención de Datos Personales de la Alcaldía Mayor de Bogotá D.C. Para mayor información consulte el [Boletín de Prensa 007 de 2019](#).

Datos personales

País de nacimiento: Número de documento:

Primer nombre: Segundo nombre:

Primer apellido: Segundo apellido:

Localidad de residencia: Dirección de residencia:

Correo electrónico: Celular:

Movilidad inteligente

¿Qué tipo de actividad realiza a diario en Bogotá?
Opción:

¿Qué medio de transporte utiliza?
Opción:

¿Qué hora de salida tiene a diario a su actividad?
Opción:

¿Qué hora de llegada tiene a diario a su actividad?
Opción:

¿Cuál es la razón principal para que te movilices en Bogotá?
Opción:

Imagen 7. Formulario Movilidad Plataforma Bogotá Cuidadora

Por su parte el formulario en la aplicación móvil GABO APP para la funcionalidad de “Registro de Movilidad” en primer lugar pide seleccionar la principal razón por la cual se da el desplazamiento y posteriormente realiza las siguientes 5 preguntas, así:

BOGOTÁ Cuidadora

Reportar Movilidad

Localidad de residencia:

Hora de salida desde el hogar:

Localidad de destino:

Hora de salida hacia el hogar:

Medio de transporte:

Guardar información

Terminos de uso e política de privacidad

Imagen 8. Formulario de Movilidad APP

Esta información es gestionada por el equipo de la Secretaría General y analizada de forma anonimizada por la Secretaría Distrital de Movilidad para la toma de decisiones informadas que propendan por el mejoramiento de las medidas de movilidad, ampliación o modificación de las rutas de Transmilenio y SITP, y el establecimiento de nuevas ciclorrutas si es pertinente.

Siguiendo la misma lógica de los anteriores formularios, el formulario de Necesito Apoyo, solicita, adicional a los datos de identificación que se describieron anteriormente el dato del estrato para identificar el tipo de ayuda del que puede ser beneficiario el solicitante así:

Por la cual se imparte una orden administrativa

VERSIÓN ÚNICA

Necesito apoyo

Registra tus datos para poder acceder a los apoyos ofrecidos por la Alcaldía en el marco de la emergencia COVID-19.

Se informa que los datos suministrados serán tratados para la identificación de población que requiere ayuda a raíz de la epidemia del covid-19.

Los datos suministrados serán tratados de conformidad con lo establecido en la [Resolución 777 de 2019](#) por medio de la cual se adopta la Política de Privacidad y Tratamiento de Datos Personales y el "Manual de Políticas y Procedimientos para el Tratamiento de Datos Personales" de la Secretaría General de la Alcaldía Mayor de Bogotá D. C.

Para mayor información consulte la Política de Privacidad de GABO APP.

Datos personales

Tipo de identificación

Selección...

Número de documento

Primer nombre

Segundo nombre

Primer apellido

Segundo apellido

Localidad de residencia

Selección...

Dirección de residencia

Cra. 54-10 - 66 Bogotá

Estado

Selección...

Fecha de nacimiento

dd/mm/aaaa

Córeo electrónico

Celular

000-000-0000

En tanto que esta funcionalidad en la aplicación móvil GABO APP no solicita datos adicionales, por lo que el usuario al acceder a esta opción únicamente debe seleccionar el tipo de ayuda que quiere pedir y hacer clic en el botón de ayuda para solicitar su gestión, así:



Imagen 10. Funcionalidad Necesito ayuda - GABO



Imagen 11. Funcionalidad Necesito ayuda - GABO

En lo que respecta al formulario de salud, el diligenciamiento de este también es voluntario para el ciudadano y se hace con el propósito de que los ciudadanos puedan reportar su estado de salud. Lo anterior, le permite a la Administración Distrital, y en concreto a la Secretaría Distrital

VERSIÓN ÚNICA

Por la cual se imparte una orden administrativa

de Salud, que es la entidad que recibe y trata directamente los datos, hacer un mejor seguimiento de la enfermedad en Bogotá e identificar ciudadanos con síntomas que puedan representar un riesgo para su propia salud y de la comunidad a la que pertenecen.

En consecuencia, además de los datos de identificación del registro, los cuales son necesarios para poder brindarle atención (conocer su nombre, dirección, teléfono para contactarlo, etc.), se piden unos campos específicos relacionados con temas de salud. Estos formularios se diseñaron tomando como referencia el estándar de registro de campos de CoronApp facilitar el intercambio y la integración con dicha App. Actualmente se trabaja con el Instituto Nacional de Salud y la Agencia Nacional Digital para que la información que se recoge por la plataforma de Bogotá Cuidadora sea integrada a la base de CoronApp.

En este punto es importante aclarar que, el formulario de Reportar Estado de Salud dispuesto en la plataforma la plataforma (sic) web www.bogota.gov.co/bogota-cuidadora enlaza a la página de la Secretaría Distrital de Salud, por lo que es esta entidad la Responsable del tratamiento de los datos para esta funcionalidad, así se aclarará al llegar al sitio de la Secretaría Distrital de Salud donde el usuario en primer lugar encuentra la Autorización de Tratamiento dispuesta por esta entidad así:

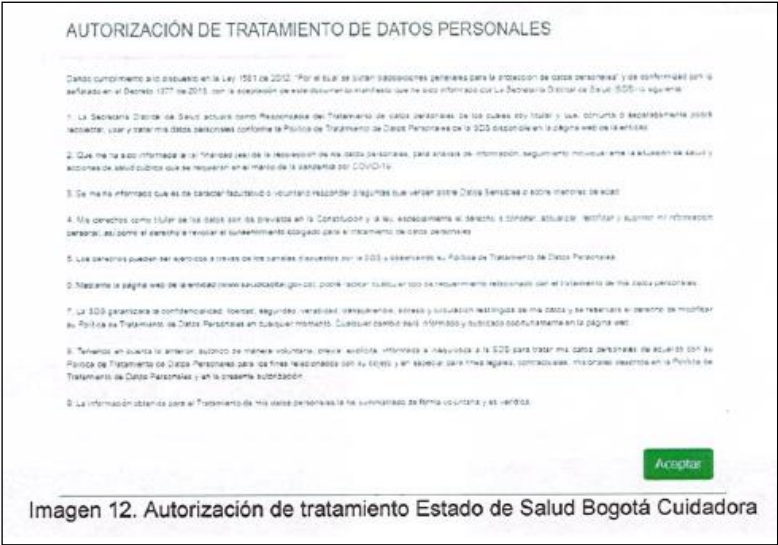


Imagen 12. Autorización de tratamiento Estado de Salud Bogotá Cuidadora

Y posteriormente se solicitan los siguientes datos:

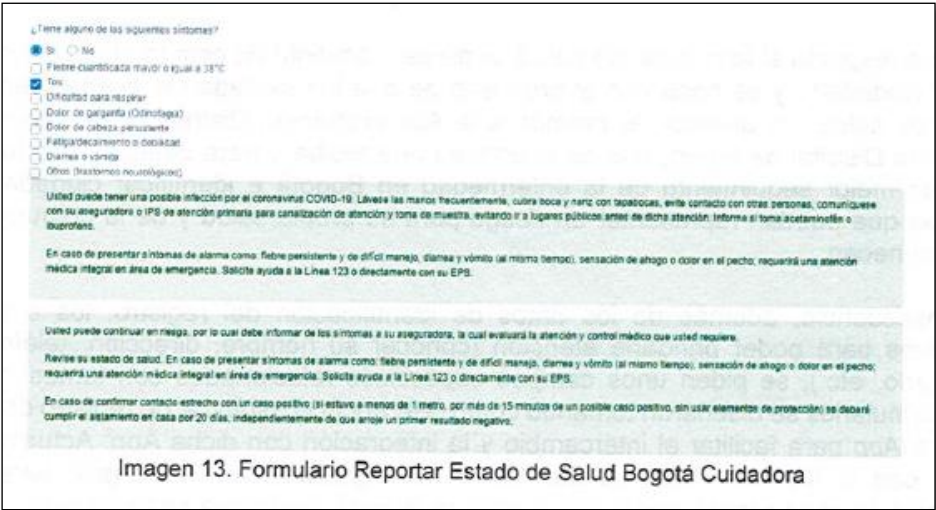


Imagen 13. Formulario Reportar Estado de Salud Bogotá Cuidadora

Por su parte en la aplicación GABO APP se solicitan los mismos datos de la pantalla anterior así:

Por la cual se imparte una orden administrativa

VERSIÓN ÚNICA

Imagen 14. Formulario Reportar Estado de Salud Gabo APP

Y si se relaciona algún síntoma de COVID 19, conforme a la integración de funcionalidades que se viene trabajando con CoronApp se despliegan menús adicionales así:

Imagen 15. Formulario Reportar Estado de Salud Gabo APP

Estas funcionalidades son fuentes de identificación de síntomas a partir del registro voluntario que éstas realizan, los datos recolectados con tratados directamente por la Secretaría Distrital de Salud para identificar zonas de concentración a partir de las cuales se pueden focalizar las acciones de búsqueda activa comunitaria.

11. Dentro de los procedimientos establecidos, ¿se tuvo en cuenta lo determinado en el artículo 6 de la Ley 1581 de 2012, en concordancia con el artículo 6 del Decreto 1377 de 2013, sobre el tratamiento de datos personales sensibles de los titulares?, en la medida que “ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles”.

Respuesta: En los formularios gestionados por la Secretaría General, a saber; los formularios de Registro de Movilidad Segura y Necesito Apoyo, no se solicitan datos sensibles de los usuarios, adicionalmente se aclara que le diligenciamiento de los formularios tanto en la aplicación Gobierno Abierto de Bogotá – GABO- como en la página web www.bogota.gov.co/bogota-cuidadora es voluntario, y así lo dejo claro el artículo 2 del Decreto 134 de 2020 que modificó el artículo 3° del Decreto 131 de 2020, el cual quedó así:

Por la cual se imparte una orden administrativa

VERSIÓN ÚNICA

"ARTÍCULO 3.- REGISTRO EN GOBIERNO ABIERTO -GABO- 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."

Conforme a todo lo anterior, es claro que el diligenciamiento de los formularios tanto en la aplicación móvil como el portal web son voluntarios por lo que de ninguna forma se condiciona al titular a suministrar datos para acceder a un servicio.

CUARTO: Que frente al tratamiento de los datos personales realizado por la Secretaría General de la Alcaldía Mayor de Bogotá D.C., a través de los aplicativos denominados "Bogotá Cuidadora" – localizado página web www.bogota.gov.co/bogota-cuidadora- y "GABO APP" esta Dirección realizó un Análisis de Vulnerabilidades a las citadas plataformas, cuyas conclusiones fueron las siguientes:

1. **"Reconfigurar de forma inmediata el servidor ["tramitesenlinea.saludcapital.gov.co"](http://tramitesenlinea.saludcapital.gov.co) puesto que expone información de carácter personal en 6 directorios, tal como se detalla en el análisis de vulnerabilidades del presente documento.**
2. **Realizar las configuraciones necesarias al servidor ["reddecuidadociudadano.gov.co"](http://reddecuidadociudadano.gov.co) para resolver las vulnerabilidades detectadas y en especial la relacionada con la navegación entre directorios que expone el contenido de 129 directorios a los cuales se puede acceder sin ningún tipo de autorización.**
3. Se deben realizar los ajustes correspondientes para resolver las vulnerabilidades reportadas para la aplicación que permite el registro de síntomas, en especial la vulnerabilidad "Cross Site Scripting" reportada con severidad alta.
4. Reemplazar el formulario utilizado para el "Registro de movilidad segura" y en su lugar implementar una solución empresarial con suficiente robustez y seguridad para el registro de los datos. Mientras se logra la implementación de esta nueva solución, se deben implementar las validaciones necesarias para asegurar el correcto diligenciamiento y asegurar que los datos ingresados sean correctos.
5. En todas las opciones que componen la plataforma web y la aplicación, se deben implementar mecanismos que permitan garantizar que la información sea registrada por los titulares de esta y evitar registro de datos erróneos, fraudulentos o sin veracidad.
6. Revisar las políticas de protección de datos de los formularios implementados con la herramienta Microsoft Forms y verificar que se autorice y vigile el envío de la información registrada a servidores ubicados fuera del país.
7. Implementar los ajustes necesarios en la aplicación GABO para que se habiliten únicamente los permisos según la funcionalidad que ofrece. El uso de permisos que no son requeridos por la aplicación genera una calificación "Critical Risk" con un puntaje de 15/100.

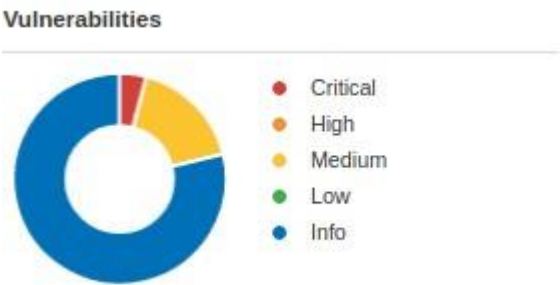
Por la cual se imparte una orden administrativa

VERSIÓN ÚNICA

8. La opción “Reportar Estado de Salud” no incluye componentes o controles que permitan al usuario ingresar su dirección o ubicación de una forma estandarizada y organizada, por lo tanto, esta aplicación no cumple con su finalidad de generar estadísticas y prevenir contagios porque se torna muy complejo ubicar en un mapa, direcciones ingresadas en un campo de texto libre.
9. Existen diferencias significativas entre la información que se captura en la aplicación y la que se registra en la plataforma web. Aunque no se conocen los detalles técnicos de estas dos soluciones, por este manejo se puede presumir que la aplicación y la plataforma web no se encuentran integradas lo cual dificulta el análisis de los datos recolectados, los cuales pueden inducir a errores en los resultados obtenidos. Al parecer las dos formas únicamente se utilizan para la recolección de datos.
10. Para facilitar el registro y análisis de la información ingresada por los ciudadanos; es necesario unificar los datos que se recolectan y las reglas de negocio que se emplean en la aplicación y la plataforma Web.
11. Revisar y ajustar los enlaces a la “Política de Tratamiento” y “Términos y Condiciones” que se muestran en el formulario de registro de la aplicación utilizada para el manejo de ayudas y que se ejecuta en el dominio “reddecuidadociudadano.gov.co” porque no muestran ningún documento.
12. Al manejar varias plataformas (Entidades), se dificulta establecer el tratamiento, las finalidades y responsabilidades para los datos personales de carácter Público, privado- semi-privado y sensibles recolectados en cada encuesta”.

Ahora bien, respecto de las conclusiones relacionadas en los numerales 1 y 2, el Análisis de Vulnerabilidades, determinó lo siguiente:

Resultado análisis servidor saludcapital.gov.co
El reporte detallado aplicado a este servidor con IP 208.30.40.188, se anexa al presente documento. En resumen, se encontraron 16 vulnerabilidades una (1) de severidad crítica, cuatro (4) de severidad media y once (11) de carácter informativo.



Adicional a la vulnerabilidad con severidad crítica que reporta la herramienta, se destaca la vulnerabilidad “Browseable Web Directories” la cual relaciona una serie de carpetas en este servidor a las cuales se puede acceder directamente y sin necesidad de una autenticación previa.

```
The following directories are browsable :  
http://208.30.40.188/servicios/  
http://208.30.40.188/servicios/login/  
http://208.30.40.188/servicios/personas/  
http://208.30.40.188/uploads/  
http://208.30.40.188/uploads/documentos/  
http://208.30.40.188/uploads/exhumacion/  
http://208.30.40.188/uploads/preliminares/  
http://208.30.40.188/uploads/rayosx/  
http://208.30.40.188/uploads/resoluciones/
```

La gravedad de esta vulnerabilidad radica en la exposición de datos personales por el tipo de documentos que se encuentran almacenados en estas carpetas dentro de los cuales aparecen: Actas de Grado y diplomas de personas naturales, Cédulas de Ciudadanía, Actas de exhumación, Resoluciones de la Entidad entre otros.

Por la cual se imparte una orden administrativa

VERSIÓN ÚNICA

208.30.40.188/uploads/

Index of /uploads

| Name | Last modified | Size | Description |
|------------------|------------------|------|-------------|
| Parent Directory | | - | |
| documentos/ | 2020-06-02 19:27 | - | |
| exhumacion/ | 2020-06-02 19:37 | - | |
| preliminares/ | 2020-06-02 18:22 | - | |
| rayosx/ | 2020-06-02 16:06 | - | |
| resoluciones/ | 2020-06-02 15:22 | - | |

Apache/2.4.18 (Ubuntu) Server at 208.30.40.188 Port 80

208.30.40.188/uploads/documentos/

Acta--20200110200942.pdf2020-01-10 20:09 428K

Acta--20200115150855.pdf2020-01-15 15:08 796K

Acta-117-20190320112508.pdf2019-03-20 10:25 120K

Acta-154-20190223115423.pdf2019-02-23 11:54 530K

Acta-591-20190314184600.pdf2019-03-14 17:46 109K

Acta-615-20190305190634.pdf2019-03-05 19:06 1.0M

Acta-615-20190308124117.pdf2019-03-08 12:41 1.0M

Acta-615-20190308124404.pdf2019-03-08 12:44 1.0M

Acta-873-20190605161531.pdf2019-06-05 15:15 275K

Acta-873-20190605164605.pdf2019-06-05 15:46 170K

Acta-1129-20200227163944.pdf2020-02-27 16:39 740K

Acta-1218-20190328131659.pdf2019-03-28 12:16 389K

Acta-1741-20190513211641.pdf2019-05-13 20:16 343K

Acta-1882-20190413111334.pdf2019-04-13 10:13 221K

BOGOTÁ

SALUD

Resolución No A 1 del día 2 del mes de del año 20

Secretaría Distrital de Salud de Bogotá D.C

Por la cual se autoriza el ejercicio de una profesión/ocupación en el Territorio Nacional.

LA SUBDIRECCIÓN INSPECCIÓN, VIGILANCIA Y CONTROL DE SERVICIOS DE SALUD

En uso de sus facultades legales y en especial las conferidas por el Decreto 780 de 2016, Ley 1164 de 2007 y Resolución 3030 de 2014 del Ministerio de Salud y Protección Social y,

CONSIDERANDO

Que el(la) señor(a) VAL EZ Identificado(a) con Cédula de ciudadanía número 13, solicitó ante esta Secretaría la autorización del ejercicio de su profesión/ocupación AUXILIAR EN ENFERMERIA otorgado por C AR, el día 20, con el acta 1, año 20.

Que estudiada la documentación presentada por el solicitante esta cumple con los requisitos establecidos en las normas legales vigentes;

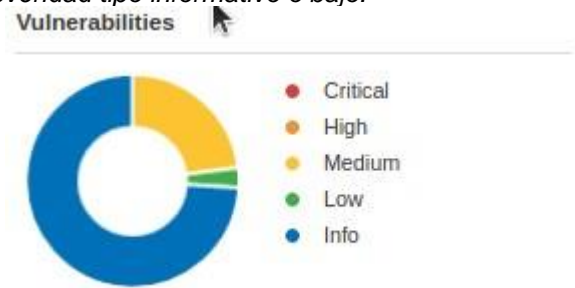
En virtud de lo expuesto este Despacho,

RESUELVE:

ARTICULO PRIMERO: Autorizar a VAL EZ Identificado(a) con Cédula de ciudadanía número 13, a ejercer la profesión/ocupación de AUXILIAR EN ENFERMERIA en el Territorio Nacional.

Resultado análisis servidor reddecuidadociudadano.gov.co

El reporte detallado aplicado a este servidor con IP 40.117.120.123, se anexa al presente documento. En resumen, se encontraron 61 vulnerabilidades, once (11) de estas con severidad media y el resto con severidad tipo informativo o bajo.



Esta herramienta detectó que el servidor tiene 129 directorios a los cuales se puede acceder sin necesidad de autenticación; aunque a simple vista estos directorios no almacenan información que contenga datos personales, esta vulnerabilidad puede afectar seriamente la aplicación que almacena.

Por la cual se imparte una orden administrativa

VERSIÓN ÚNICA

Output

```
The following directories are browsable :  
  
https://40.117.120.123/css/  
https://40.117.120.123/css/demos/  
https://40.117.120.123/css/fonts/  
https://40.117.120.123/css/skins/  
https://40.117.120.123/img/  
https://40.117.120.123/img/about/  
https://40.117.120.123/img/animated/  
https://40.117.120.123/img/avatars/  
https://40.117.120.123/img/backgrounds/  
https://40.117.120.123/img/banner/  
https://40.117.120.123/img/blog/  
https://40.117.120.123/img/blog/default/  
https://40.117.120.123/img/blog/large/  
https://40.117.120.123/img/blog/medium/  
https://40.117.120.123/img/blog/small/  
https://40.117.120.123/img/blog/square/  
https://40.117.120.123/img/blog/wide/  
https://40.117.120.123/img/buttons/  
https://40.117.120.123/img/clients/  
https://40.117.120.123/img/demos/  
https://40.117.120.123/img/demos/app-landing/  
https://40.117.120.123/img/demos/architecture-interior/  
https://40.117.120.123/img/demos/band/  
https://40.117.120.123/img/demos/barber/  
https://40.117.120.123/img/demos/business-consulting/  
https://40.117.120.123/img/demos/church/  
https://40.117.120.123/img/demos/coffee/  
https://40.117.120.123/img/demos/construction/  
https://40.117.120.123/img/demos/digital-agency/
```

Como puede observarse las conclusiones descritas en los numerales 1 y 2 ponen de presente que en los servidores **tramitesenlinea.saludcapital.gov.co** y **reddecuidadociudadano.gov.co** se exponen directorios que pueden poner en riesgo la integridad, disponibilidad y confidencialidad de la información allí almacenada, la cual corresponde al registro de los formularios “Estado de Salud” y “Ofrezco Ayuda”, respectivamente.

Lo anterior es inconsistente con el principio y el deber de seguridad de la información previsto en la norma citada y en el literal d) del artículo 17 de la Ley Estatutaria 1581 de 2012, que ordena lo siguiente:

*“ARTÍCULO 17. DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO. Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:
(...)*

*d) Conservar la información bajo las **condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento**; (...)* (Destacamos)

Así las cosas, de conformidad con lo establecido en el literal g) del artículo 4 de la Ley 1581 de 2012, *“la información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento”*; Por eso, **los Responsables del tratamiento tienen el deber de “conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento”**, de acuerdo con lo dispuesto en el literal d) del artículo 17 de la Ley 1581 de 2012.

En referencia a lo anterior, 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’”²

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 las medidas necesarias y efectivas 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

² 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.).

Por la cual se imparte una orden administrativa

VERSIÓN ÚNICA

de seguridad de naturaleza humana, física, administrativas, técnicas y de cualquier otra índole que refuercen las anteriores medidas.

Ahora, si bien existen unos procedimientos y medidas implementadas por la Secretaría General de la Alcaldía Mayor de Bogotá D.C., en su calidad de Responsable para **evitar** incidentes relacionados con transgresiones a los protocolos de seguridad adoptados, pueden presentarse fallas que incrementen los riesgos sobre la información que ha sido recolectada y almacenada en sus bases de datos.

Las medidas de seguridad deben estar dirigidas a evitar que se presente cualquier tipo de irregularidad que, entre otras, facilite o permita que, por ejemplo se acceda a los datos personales de otras personas, situación que adquiere mayor importancia, sí se tiene en cuenta la existencia de datos de carácter sensible.

Por lo tanto, las actividades tendientes a mitigar posibles fallas en las medidas de seguridad adoptadas deben tener un carácter permanente y ser monitoreadas para establecer su pertinencia y efectiva protección de los datos personales.

QUINTO: DEL DEBER DE CONSERVAR LA INFORMACIÓN BAJO CONDICIONES DE SEGURIDAD.

De conformidad con lo establecido en el literal g) del artículo 4 de la Ley 1581 de 2012, *“la información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento”*; Por eso, **los Responsables del tratamiento tienen el deber de “conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento”**, de acuerdo con lo dispuesto en el literal d) del artículo 17 de la Ley 1581 de 2012.

Nótese que **la redacción del principio de seguridad tiene un criterio eminentemente preventivo**, lo cual obliga a los Responsables o Encargados a adoptar medidas apropiadas y efectivas para **evitar** afectaciones a la seguridad de la información sobre las personas.

Proteger la información es una condición crucial del tratamiento de datos personales. Una vez recolectada debe ser objeto de medidas de diversa índole para evitar situaciones indeseadas que pueden afectar los derechos de los titulares y de los mismos responsables y encargados del tratamiento. El acceso, la consulta y el uso no autorizado o fraudulento, así como la manipulación y pérdida de la información son los principales riesgos que se quieran mitigar a través de las medidas de seguridad de naturaleza humana, física, administrativa, técnica o de cualquier otra índole.

Del texto del precitado artículo 17 de la Ley Estatutaria 1581 de 2012 se concluye, entre otras, que las medidas de seguridad deben estar dirigidas a evitar que se presente cualquier tipo de irregularidad que, entre otras, facilite o permita que una persona no autorizada un acceda a los datos personales de otras personas, situación que adquiere mayor importancia, sí se tiene en cuenta la existencia de datos de carácter sensible.

Por lo tanto, las actividades tendientes a mitigar posibles fallas en las medidas de seguridad adoptadas deben tener un carácter permanente y ser monitoreadas para establecer su pertinencia y efectiva protección de los datos personales.

SEXTO: DEL TRATAMIENTO DE DATOS SENSIBLES

Los datos sensibles son aquellos que por su naturaleza están relacionados con aspectos muy íntimos de la persona o que pueden ser nicho de discriminaciones o comprometer los derechos y libertades de las personas. Por esta razón, el artículo 6 de la ley 1581 de 2012 prohíbe, como regla general, el tratamiento de esa clase de información. En otras palabras, el tratamiento de datos sensibles es excepcionalmente permitido.

Por la cual se imparte una orden administrativa

VERSIÓN ÚNICA

Los datos sensibles fueron definidos en la ley 1581 de 2012 y en el decreto 1377 de 2013³ como “aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos”⁴. Para la Corte Constitucional la anterior lista de ejemplos de información sensible no debe considerarse como taxativa “sino meramente enunciativa de datos sensibles, pues los datos que pertenecen a la esfera íntima son determinados por los cambios y el desarrollo histórico”⁵

En el Tratamiento de datos personales sensibles, cuando dicho Tratamiento sea posible conforme a lo establecido en el artículo 6 de la Ley 1581 de 2012, deberán cumplirse las siguientes obligaciones:

1. **Informar al titular que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento.**
2. **Informar al titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de Tratamiento son sensibles y la finalidad del Tratamiento, así como obtener su consentimiento expreso.**

Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles.” (Destacamos)

Adicionalmente, 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**”⁶

SÉPTIMO: RESPONSABILIDAD DEMOSTRADA (ACCOUNTABILITY) EN EL TRATAMIENTO DE DATOS PERSONALES

La regulación colombiana le impone al Responsable del Tratamiento, la responsabilidad de adoptar las medidas necesarias para cumplir la Ley 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). 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*”⁷.

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.

El artículo 26⁸ -Demostración- establece que, “*los responsables [sic] del tratamiento [sic] de datos [sic] personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y*

³ Norma compilada en el Decreto Único Reglamentario 1074 de 2015.

⁴ Artículo 5 de la ley 1581 de 2012, repetido en el numeral 3 del artículo 3 del decreto 1377 de 2013

⁵ Cfr. Corte Constitucional, sentencia C-748 de 2011, numeral 2.7.3

⁶ Cfr. Corte Constitucional, sentencia C-748 de 2011, numeral 2.8.4

⁷ Cfr. Corte Constitucional, sentencia T-227 de 2003.

⁸ El texto completo del artículo 26 del Decreto 1377 de 2013 ordena: “*Demostración. Los responsables [sic] del tratamiento [sic] de datos [sic] personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado*

Por la cual se imparte una orden administrativa

VERSIÓN ÚNICA

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"*⁹ (*accountability*)¹⁰.

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 ese análisis, las recomendaciones que trae la guía a los obligados a cumplir la Ley 1581 de 2012, son:

1. 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;
2. Desarrollar un plan de revisión, supervisión, evaluación y control del PIGDP; y
3. Demostrar el debido cumplimiento de la regulación sobre Tratamiento de Datos personales.

El Principio de Responsabilidad Demostrada –*accountability*– demanda implementar acciones de diversa naturaleza¹² 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.

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 [sic] 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 [sic] personales objeto del tratamiento [sic].
3. El tipo de Tratamiento.
4. Los riesgos potenciales que el referido tratamiento [sic] podrían causar sobre los derechos de los titulares [sic].

En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, los Responsables deberán suministrar a esta una descripción de los procedimientos usados para la recolección de los datos [sic] personales, como también la descripción de las finalidades para las cuales esta información es recolectada y una explicación sobre la relevancia de los datos [sic] personales en cada caso.

En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, quienes efectúen el Tratamiento de los datos [sic] personales deberán suministrar a esta evidencia sobre la implementación efectiva de las medidas de seguridad apropiadas"

⁹ El texto de la guía puede consultarse en: <http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf>

¹⁰ "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.

¹¹ Cfr. Grupo de trabajo de protección de datos del artículo 29. Dictamen 3/2010 sobre el principio de responsabilidad, pág. 8.

¹² Estas medidas pueden ser de naturaleza administrativa, organizacional, estratégica, tecnológica, humana y de gestión. Asimismo, involucran procesos y procedimientos con características propias en atención al objetivo que persiguen.

Por la cual se imparte una orden administrativa

VERSIÓN ÚNICA

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 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**”*¹³. (Énfasis añadido).

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.

La identificación y clasificación de riesgos, así como la adopción de medidas para mitigarlos son elementos cardinales del Principio de Responsabilidad Demostrada (*accountability*). En la mencionada guía se considera fundamental que las organizaciones desarrollen y ejecuten, entre otros, un *“sistema de administración de riesgos asociados al tratamiento [sic] de datos [sic] personales”*¹⁴ que les permita *“identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos en desarrollo del cumplimiento de las normas de protección de datos personales”*¹⁵.

CONCLUSIONES:

1. De conformidad con lo establecido en el Manual de Políticas y Procedimientos para el Tratamiento de Datos Personales adoptado mediante Resolución 777 del 18 de diciembre de 2019, la Secretaría General de la Alcaldía Mayor de Bogotá D.C. es el Responsable del tratamiento de los datos que se recolectan a través de las plataformas www.bogota.gov.co/bogota-cuidadora- y “GABO APP”.
2. Las plataformas www.bogota.gov.co/bogota-cuidadora- y “GABO APP, utilizan los servidores tramitesenlinea.saludcapital.gov.co y reddecuidadociudadano.gov.co para almacenar el registro de los formularios “Estado de Salud” y “Ofrezco a Ayuda”, respectivamente.
3. El Análisis de Vulnerabilidades realizado por esta Dirección, a los citados servidores, arrojó como resultado que existen **fallas de seguridad o falencias** que ponen en riesgo la seguridad de la información que es recolectada, así:
 - a) Respecto del servidor tramitesenlinea.saludcapital.gov.co, la exposición de 6 directorios o carpetas que contienen datos personales, y a los cuales es posible acceder sin autorización. **La gravedad de esta vulnerabilidad radica en la exposición de datos personales por el tipo de documentos que se encuentran almacenados en estas carpetas dentro de los cuales aparecen: Actas de Grado y diplomas de personas naturales, Cédulas de Ciudadanía, Actas de exhumación, Resoluciones de la Entidad entre otros.**
 - b) En lo que tiene que ver con el servidor reddecuidadociudadano.gov.co, se encontró igualmente que es posible acceder a otros directorios o carpetas sin tener autorización o

¹³ 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 internamente realicen las organizaciones y definan en sus políticas o regulaciones internas.

¹⁴ Cfr. Superintendencia de Industria y Comercio (2015) “Guía para implementación del principio de responsabilidad demostrada (*accountability*)”, págs 16-18.

¹⁵ *Ibidem*.

Por la cual se imparte una orden administrativa

sin que pida autenticación para ello, poniendo en riesgo la información que es almacenada en este servidor.

- Mediante la aplicación GABO APP se solicita información relacionada al estado de salud de las personas, la cual es considerada como datos sensibles (artículo 5 de la Ley Estatutaria 1581 de 2012).

Así las cosas, esta Dirección impartirá órdenes administrativas, para que, la Secretaría General de la Alcaldía Mayor de Bogotá D.C., en su calidad de Responsable del tratamiento de los datos personales recolectados o tratados en las plataformas www.bogota.gov.co/bogota-cuidadora- y “GABO APP: (1) implemente mecanismos eficientes y eficaces para evitar accesos no autorizados o se descargue la información recolectada a través de dichas plataformas; (2) Fortalezca las medidas de seguridad, acceso y uso limitado, circulación restringida y confidencialidad de los datos sensibles.

En mérito de lo expuesto, esta Dirección

RESUELVE

ARTÍCULO PRIMERO: ORDENAR a la Secretaría General de la Alcaldía Mayor de Bogotá D.C., identificada con el NIT. 899.999.061-9, que implemente las medidas de seguridad apropiadas y efectivas para impedir el acceso o descarga de la información recolectada y tratada en las plataformas denominadas “Bogotá Cuidadora” y “GABO APP”, en especial en los servidores tramitesenlinea.saludcapital.gov.co y reddecuidadociudadano.gov.co de conformidad con la parte considerativa del presente acto administrativo; medidas que deben venir acompañadas de mecanismos de monitoreo y control que permitan la debida protección de la información tratada.

ARTÍCULO SEGUNDO: ORDENAR a la Secretaría General de la Alcaldía Mayor de Bogotá D.C., identificada con el NIT. 899.999.061-9, que fortalezca las medidas de seguridad, acceso y uso limitado, circulación restringida y confidencialidad de los datos sensibles, de tal forma que no sólo implemente la “*responsabilidad demostrada*” sino la “*responsabilidad reforzada*”, la cual, según la Corte Constitucional se traduce en una exigencia mayor en términos de cumplimiento de los principios del artículo 4 y los deberes del título VI de la Ley Estatutaria 1581 de 2012.

ARTÍCULO TERCERO: La Secretaría General de la Alcaldía Mayor de Bogotá D.C. deberá cumplir lo ordenado en esta resolución dentro de los diez (10) días siguientes a la ejecutoria del presente acto administrativo.

PARÁGRAFO: Para demostrar el cumplimiento deberá remitir una certificación suscrita por la Secretaría General de la Alcaldía Mayor de Bogotá D.C., en su calidad de Responsable del Tratamiento con la cual se acredite y evidencie la implementación de las medidas ordenadas.

ARTÍCULO CUARTO: Notificar el contenido del presente acto administrativo a la Secretaría General de la Alcaldía Mayor de Bogotá D.C., informándole que contra el presente acto administrativo procede recurso de reposición ante el Director de Investigación de Protección de Datos Personales 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., 05 AGOSTO 2020

El Director de Investigación de Protección de Datos Personales,

CARLOS ENRIQUE SALAZAR MUÑOZ

Por la cual se imparte una orden administrativa

VERSIÓN ÚNICA

NOTIFICACIÓN:

| | |
|----------------------|---|
| Entidad: | SECRETARÍA GENERAL ALCALDÍA MAYOR DE BOGOTÁ D.C. |
| NIT.: | 899.999.061-9 |
| Representante Legal: | MARGARITA BARRAQUER SOURDIS |
| Identificación | C.C. 39.776.077 |
| Dirección: | Carrera 8 número 10 – 65 |
| Ciudad: | Bogotá D.C. – Colombia |
| Correo electrónico: | <u>notifica.judicial@gobiernobogota.gov.co</u> |