REPÚBLICA DE COLOMBIA

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

RESOLUCIÓN NÚMERO 47703 DE 2020

(18 AGOSTO 2020)

Por la cual se imparten unas ordenes administrativas

Radicación 20-155849

VERSIÓN ÚNICA

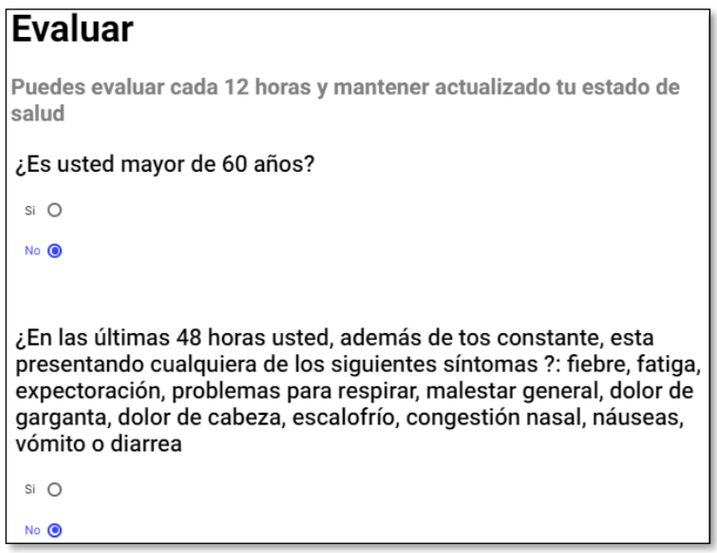
EL DIRECTOR DE INVESTIGACIÓN DE PROTECCION DE DATOS PERSONALES

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

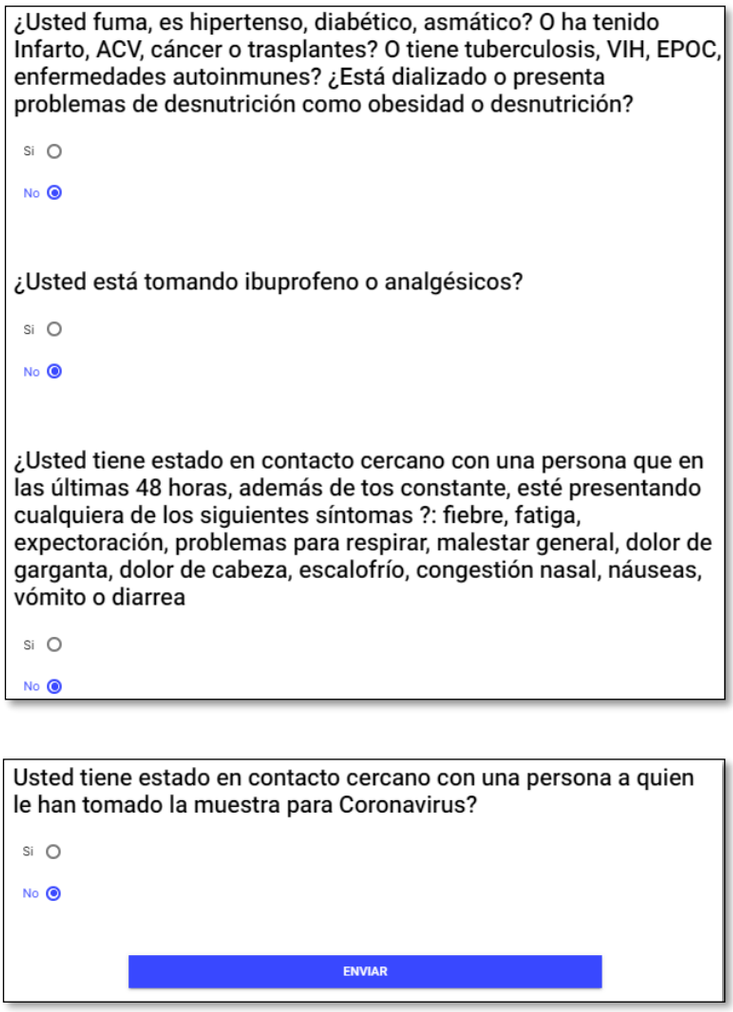
CONSIDERANDO:

PRIMERO: Que "ValleCorona" https://www.vallecorona.com/ no sólo es la plataforma oficial del Valle del Cauca para afrontar el Covid19, sino una aplicación móvil (App) utilizada para dicho efecto. Mediante esas herramientas, la GOBERNACIÓN DEL VALLE DEL CAUCA permite al Departamento del Valle de Cauca mantener a*"(. . .) todas las personas contagiadas (. . .) identificadas y georreferenciadas (. . .)"* así como *(. . .) la ubicación del paciente (. . .)"*[1]. Para el efecto, se recolecta la siguiente información de los Titulares que desean usar la aplicación: (i) Tipo de identificación; (ii) número de identificación; (iii) nombres y apellidos; (iv) país de nacionalidad; (v) género y fecha de nacimiento; (vi) correo electrónico; (vii) dirección; (viii) EPS; (ix) Ocupación; (x) indicación de la cantidad de personas con las que habita el Titular.

Así mismo, en el enlace de "Autoevaluación", se solicitan datos inherentes a la salud de la persona que vaya a inscribirse, así:



[1] Mónica Rojas y Martha Cecilia Bocanegra, "En Cali comienza el seguimiento inteligente a pacientes del COVID-19", Portal de noticias Alcaldía de Cali (Jun. 2, 2020, 2:46 PM), https://www.cali.gov.co/salud/publicaciones/152949/en-cali-comienza-el-seguimiento-inteligente-a-pacientes-covid-19/.



SEGUNDO: Que en razón de lo anterior, esta Dirección requirió en dos (2) oportunidades a la Gobernación del Valle del Cauca[2] y a la Alcaldía de la Ciudad de Cali[3], para que dieran respuesta a las siguientes preguntas:

(1) *Entre la fecha de implementación efectiva del aplicativo denominado "Cali Valle Corona" a la fecha del presente requerimiento ¿cuántas personas se han inscrito o registrado en ella?*

(2) *Informe si la recolección y el tratamiento de los datos que se obtengan a través del aplicativo denominado "Cali Valle Corona" se realiza directamente por parte de la Alcaldía de Cali, o alguna de sus dependencias, o bien, a través de los servicios de un tercero ("Encargado del Tratamiento") para que se encargue de todos los aspectos relativos al tratamiento de datos personales. En caso afirmativo de acudir a los servicios de un tercero, remita copia del contrato celebrado con este tercero.*

(3) *Informe si durante el período de diseño, desarrollo y de recolección de datos del aplicativo denominado "Cali Valle Corona" se realizó un estudio de impacto de privacidad ("Privacy Impact Assessment" o "PIA", por sus siglas en inglés). En caso afirmativo, remita copia completa de dicho estudio.*

(4) *Informe si se realizó una evaluación de los riesgos específicos para los derechos y libertades de los Títulares de los Datos Personales a efectos la implementación del aplicativo denominado "Cali Valle Corona". En caso afirmativo, remita copia completa de dicha evaluación.*

[2] Los requerimientos se hicieron bajo los radicados 20-155849-0 del 3 de junio de 2020 y 20-155849-1 del 24 de junio de 2020.
[3] Los requerimientos se hicieron bajo los radicados 20-155788-0 del 3 de junio de 2020 y 20-155788-1 del 24 de junio de 2020.

(5) Informe si se desarrollo y puso en ejecución un Sistema de Administración de Riesgos asociados al Tratamiento de Datos Personales que les permita "identificar, medir, controlar y mointorear" todos aquellos situaciónes que puedan incidir en la debida administración del riesgo a que están expuestos los ciudadanos por causa u ocasión del tratamiento de sus datos a través del aplicativo denominado "Cali Valle Corona" localizada en la página web https://app.calivallecorona.com . En caso afirmativo, remita copia del documento.

(6) Informe que medidas tecnológicas, humanas, administrativas, físicas, contractuales y de cualquier otra índole han implementado para que 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, y;
(e) Circulación o suministro de la información a personas no autorizadas.

(7) Informe si esas medidas de seguridad son objeto de revisión, evaluación y mejora permanente;

(8) De conformidad con lo establecido en el D. 1377/13 -compilado en el D.1074/15-, atendiendo las limitaciones temporales en el tratamiento de datos personales ¿tiene la Alcaldía de Cali establecido el procedimiento para la supresión de la información que sea recolectada en el portal https://app.calivallecorona.com?"

TERCERO: Que frente a los anteriores interrogantes, únicamente dio respuesta la Gobernación del Valle del Cauca, a través de su Secretario de las TIC, mediante Oficio radicado con el número 20-155849-5 de fecha 2 de julio de 2020, en los siguientes términos:

"En lo que respecta al desarrollo de la aplicación "VALLECORONA", conviene mencionar que, con ocasión a la contingencia generada por la propagación del nuevo Coronavirus COVID-19, la cual fue decretada mediante la Resolución 385 del 12 de marzo de 2020, de conformidad con lo establecido en el artículo 69 de la Ley 1753 de 2015, La Secretaría de Salud del Valle del Cauca ve la necesidad de recurrir a la ayuda tecnológica, a través del uso de una aplicación que permitiera tener información en tiempo real de los posibles casos COVID-19 positivos, llevar a cabo un seguimiento demográfico de los casos registrados como positivos presentes en el territorio del Departamento del Valle del Cauca, así como incluir funcionalidades que permitieran tanto al departamento como a los municipios que lo conforman, gestionar la movilidad de los ciudadanos para la reactivación de las empresas que pertenecen a los sectores de industria y comercio autorizados por el Gobierno Nacional, monitorear el tránsito de las personas y detectar los ciudadanos diagnosticados COVID-19 Positivos que están circulando y violando la restricción de salida por su condición de salud.

Es por lo anterior que se aúnan esfuerzos con el sector privado, quienes a título gratuito, le apuestan a la iniciativa desarrollando dicha plataforma, la cual fue publicada en su primera versión en la tienda de aplicación de Android, vinculada a la Alcaldía de Santiago de Cali, dado que dicha entidad se configuraba como la primer usuaria de las funcionalidades que la plataforma digital ofrecía.

Dado el aumento exponencial de casos COVID-19 en el Departamento del Valle del Cauda y la necesidad de trabajar mancomunadamente con los municipios, para lograr una cobertura amplía a nivel departamental, se acuerda trasladar el desarrollo de la aplicación "CaliValleCorona" a la Gobernación del Valle del Cauca en conjunto con las empresas del sector privado, motivo por el cual la App modifica su nombre a "ValleCorona", siendo este más inclusivo respecto de todo el territorio del departamento y se reubica en la tienda de aplicaciones de Android, vinculada a la Gobernación del Valle del Cauca. *(negrilla fuera de texto)*

En tal sentido, resulta fundamental exponer que la aplicación "ValleCorona App", alimenta sus bases de datos, mediante la información proporcionada por la Secretaría de Salud Departamental, los usuarios que acceden a la misma a través de su descarga en la tienda de aplicaciones de Android, las EPD a nivel Departamental, la Gobernación del Valle del Cauca a través de sus canales de atención al público y alcaldías municipales actuando mediante sus respectivas Secretarías de Salud.

(1) "Entre la fecha de implementación efectiva del aplicativo denominado "Cali Valle Corona" a la fecha del presente requerimiento ¿cuántas personas se han inscrito o registrado en ella?

Respuesta:

En la base de datos de "ValleCorona", a la fecha de 25 de junio de 2020 se encuentran 69.332 usuario registrados.

(2) Informe si la recolección y el tratamientos de los datos que se obtengan a través del aplicativo denominado "Cali Valle Corona" se realiza directamente por parte de la Gobernación del Valle del Cauca, o alguna de sus dependencias, o bien, a través de los servicios de un tercero ("Encargado del Tratamiento") para que se encargue de todos los aspectos relativos al tratamiento de datos personales. En caso afirmativo de acudir a los servicios de un tercero, remita copia del contrato celebrado con este tercero.

Respuesta:

Inicialmente la empresa HelpPeople, mediante carta de intención dirigida a la Secretaria de Salud Departamental ofreció un grupo de desarrolladores para implementar la aplicación en el resto del departamento. La Secretaría de Salud Departamental solicitó concepto técnico a la Secretaría de las TIC, por ser esta la encargada de dar viabilidad y posterior utilización de la aplicación en el Departamento.

La Secretaría TIC emitió concepto técnico viable sobre la utilización de la aplicación bajo estricto cumplimiento del manual de políticas TIC del Departamento, numerales 5.2. Políticas y estándares de seguridad personal , 5.4 políticas y estándares de cumplimiento de seguridad informática, 5.4.1 derechos de propiedad intelectual, 5.4.3. violación de seguridad informática, 5.7.7. manejo de base de datos, y 5.5. políticas generales, de esta manera se suscribe un acuerdo de confidencialidad y un acuerdo de transmisión y manejo de datos personales entre las partes.

Para la implementación de la aplicación "ValleCorona" en el Valle del Cauca, la Secretaría de Salud Departamental aportó la base de datos inicial cumpliendo con el numeral 5.7.7. manejo de base de datos del manual de políticas TIC.

HelpPeople en su calidad de tercero "encargado del tratamiento", realiza la recolección y tratamiento de los datos personales almacenados en la aplicación ValleCorona (se adjuntan: Acuerdo de confidencialidad y acuerdos de transmisión de datos y manejo de datos personales).

(3) Informe si durante el período de diseño, desarrollo y de recolección de datos del aplicativo denominado "Cali Valle Corona" se realizó un estudio de impacto de privacidad ("Privacy Impact Assessment" o "PIA", por sus siglas en inglés). En caso afirmativo, remita copia completa de dicho estudio.

Respuesta:

Para la implementación de la aplicación "Valle Corona", se realizó un EIPD (Evaluación de Impacto en la protección de datos personales), el cual se anexa al presente documento de respuesta.

(4) Informe si se realizó una evaluación de los riesgos específicos para los derechos y libertades de los Títulares de los Datos Personales a efectos la implementación del aplicativo denominado "Cali Valle Corona". En caso afirmativo, remita copia completa de dicha evaluación.

Respuesta:

Para la implementación de la aplicación "ValleCorona", se realizó una matriz de riesgos, el cual se anexa al presente documento de respuesta.

(5) Informe si se desarrollo y puso en ejecución un Sistema de Administración de Riesgos asociados al Tratamiento de Datos Personales que les permita "identificar, medir,

controlar y mointorear" todos aquellos situaciónes que puedan incidir en la debida administración del riesgo a que están expuestos los ciudadanos por causa u ocasión del tratamiento de sus datos a través del aplicativo denominado "Cali Valle Corona" localizada en la página web https://app.calivallecorona.com. En caso afirmativo, remita copia del documento.

Respuesta:

Para los datos personales almacenados en la base de datos de la aplicación "ValleCorona", se implementaron medidas de seguridad para identificar, medir, controlar y monitorear ambas interfaces de usuario: la app móvil y el acceso web hhtps://app.calivallecorona.com, en ambos casos aplica la misma matriz de riesgos, debido a que a alimenta la misma base de datos.

(6) Informe que medidas tecnológicas, humanas, administrativas, físicas, contractuales y de cualquier otra índole han implementado para que 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, y;
e) Circulación o suministro de la información a personas no autorizadas.

Respuesta:

En cumplimiento del principio de seguridad, a continuación, se relacionan las medidas implementadas, las cuales también se relacionan en la matriz de riesgos:

Medidas Técnicas:

- *Restricciones de acceso a los sistemas de información con perfilamiento de usuarios.*
- *Ningún usuario puede descargar información.*
- *Se cuenta con un firewall que está en frente de toda la solución y la información que se expone en internet.*
- *Se implementaron controles técnicos de seguridad a la infraestructura donde se encuentra la base de datos de ValleCorona.*
- *Se cuenta con backups distribuidos tanto de la máquina con la base de datos.*
- *Se cuenta con un sistema de información donde se registran los incidentes de seguridad (HelpPeople Service Management).*
- *Se cuenta con un servicio de tolerancia que provee AWS con servidores redundantes en diferentes datacenters.*
- *Seguridad lógica implementada (firewall) para minimizar los ataques de DDOS (denegación de servicio).*
- *Se cuenta con UPS que soporta los cortes eléctricos temporales,*
- *Se cuenta con canales de internet (principal y backups),*
- *Se cuenta con logs de acceso y modificación.*
- *Se cuenta con visores de eventos en la Base de datos.*
- *Para la integración de la base de datos del INS con Vallecorona, se cuenta con un equipo de personas que realizan la depuración y calidad del dato antes de realizar la integración.*
- *Se cuenta con restricción de acceso a los sistemas de información con perfilamiento de usuarios.*

Medidas Humanas:

- *Se han realizado capacitaciones en protección de datos personales al grupo de interesados que tienen acceso a la base de datos.*
- *Se cuenta con asesores expertos en protección de datos personales, los cuales se encargan de garantizar el cumplimiento de la ley 1581 de 2012 y sus decretos reglamentarios.*

Medidas administrativas:

- *Se cuenta con acuerdo de transmisión y tratamiento de datos personales y acuerdo de confidencialidad entre la secretaria de saludo, secretaría TIC y el Help People quien es el encargado del manejo de los datos.*
- *Se cuenta con políticas y procedimientos de seguridad de la información y de protección de datos personales por parte de la gobernación del Valle del Cauca y de parte de Help People.*

- *Se realizó un EIPD (Evaluación de Impacto de Protección de Datos).*
- *Se realizó una matriz de riesgos para identificar los riesgos inherentes asociados al tratamiento de datos personales y los controles implementados al mismo.*
- *Se registró la base de datos ValleCorona en la SIC bajo el radicado 20-172434-000000-000.*

En los términos y condiciones de uso de la app, se informa en canal de atención, en el apartado "Tratamiento de datos personales." Adicionalmente en la Play Store y en la app se direcciona a la política de tratamiento de datos personales de la Gobernación del Valle del Cauca la cual contiene el procedimiento para que el titular de los datos pueda ejercer sus derechos de hábeas data.

(7) Informe si esas medidas de seguridad son objeto de revisión, evaluación y mejora permanente.

Respuesta:

Desde la salida en vigencia de la aplicación "ValleCorona" a la fecha, se realiza monitoreos programados a las medidas técnicas , administrativa y humanas, en función de brindar protección a la información. Adicionalmente se realizan mejoras continuas a la aplicación "ValleCorona", las cuales se evidencian en las versiones publicadas en la PlayStore.

(8) De conformidad con lo establecido en el D. 1377/13 -compilado en el D.1074/15-, atendiendo las limitaciones temporales en el tratamiento de datos personales ¿tiene la Gobernación del Valle del Cauca establecido el procedimiento para la supresión de la información que sea recolectada en el portal https://app.calivallecorona.com?"

Respuesta:

La gobernación del Valle del Cauca en cabeza de la secretaria de salud y la secretaría TIC en conjunto con el encargado el tratamiento HelpPeople, definirán el procedimiento para anonimizar los datos personales y conservar la información estadística relevante siguiendo los parámetros dictados por la superintendencia de industria y comercio en atención al artículo 2.2.2.25.2.8 del decreto 1074/15.

Se tiene establecido que: una vez finalizada la declaración de Emergencia Sanitaria (Resolución 385 de 12 de marzo de 2020 y el Decreto 417 de 2020), los datos serán anonimizados, de tal forma que se pueda evitar que una persona sea identificada o identificable a través de algún dato de los ya capturados. Los datos que se conservarán, los cuales no apuntarán a ninguna persona en específico, serán utilizados con fines estadísticos, datos abiertos e información que tanto la Secretaria de Salud Departamental como el Ministerio de Salud, requieran para sus diferentes estudios epidemiológicos, datos históricos y base de conocimiento para enfrentar posibles futuras epidemias.

(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, es pertinente y adecuada para la finalidad descrita en el documento "términos y condiciones para el uso de la plataforma https://app.calivallecorona.com"?

Respuesta:

Para la definición de los datos personales solicitados en el sitio web, se tuvieron en cuenta los siguientes resoluciones y decretos expedidos por el Gobierno Nacional:

- *Resolución 385 del 12 de marzo de 2020, el ministerio de salud y protección social, de acuerdo con lo establecido en el artículo 69 de la Ley 1753 de 2015, declaró el estado de emergencia sanitaria por causa del nuevo coronavirus COVID-19 en todo el territorio nacional hasta el 30 de mayo de 2020.*
- *Decreto 417 de 2020, con el fin de conjurar la grave calamidad pública que afecta al país por causa del nuevo coronavirus COVID-19.*
- *Decreto 614 del 30 de abril de 2020 – aplicación de tecnología para tener acceso a información sobre emergencias sanitarias, su evolución en el país, alertas de prevención y reportar autodiagnóstico de salud.*

- *Resolución 666 del 24 de abril de 2020 – Se deben implementar medidas de bioseguridad y controles.*
- *Circular 001 del 23 de marzo de 2020 – Hace mención a la excepción de solicitud de autorización de datos personales por parte del Titular por caso de emergencia médica y sanitaria. Artículo 10 letra c, Articulo 10 y 13 de la Ley 1581 de 2012.*
- *Resolución 464 del 18 de marzo de 2020 - Obligatoriedad de aplicar el aislamiento preventivo para proteger a los adultos mayores de 70 años.*
- *Decreto 636 de 6 de mayo de 2020 – Se imparten instrucciones en virtud de la emergencia sanitaria generada por la pandemia del Coronavirus COVID-19, y el mantenimiento del orden público.*

Adicionalmente, atendiendo la necesidad de reactivación de la economía, a las necesidades de la ciudadanía de estar informada y de recibir atención médica y psicológica, a las necesidades de las Entidades de Salud Departamental y Municipal, se definió el tipo de información a recolectar que permitiría las necesidades ya expuestas. A continuación, se informa el tipo de datos recolectados:

- *Número telefónico: para envío de mensajes de texto de confirmación y para las llamadas del servicio de atención de bienestar emocional.*
- *Datos de identificación, ubicación, y contacto: Nombre, cédula, número telefónico, dirección de vivienda, dirección del sitio de trabajo, correo electrónico para diferentes servicios tales como: Gestión del permiso de movilidad, gestión de citas médicas, línea de atención de bienestar emocional.*
- *Datos de afiliación: EPS, para notificar si es el caso a las entidades correspondientes.*
- *Datos de la compañía en la que labora el ciudadano (Titular de los datos) para gestionar el permiso de movilidad.*
- *Datos relacionados con el estado de salud de la persona: Para identificar si la persona Covid-19 positivo o tiene síntomas relacionados con el virus mencionado.*
- *Datos de geolocalización y actividad física: Los datos de geolocalización se toman para identificar el rango de movilidad y posible contagio de las personas portadoras del COVID-19. Se busca mitigar, controlar la propagación del COVID.*
- *Los datos de actividad física son un requisito para identificar cuando la persona inicia su movilidad cuando está fuera de la geocerca. Dando cumplimiento también a la Resolución 464 de 2000 y el Decreto 636 de 2020.*
- *Dentro de los permisos se solicita la app está el uso de la cámara para ser utilizado por el módulo puesto de control. En este modulo se utiliza la cámara para escanear el código de barras de los documentos de identidad y comparar estos datos con la información almacenada en la base de datos y así identificar si un ciudadano covid positivo estña transitando libremente en las calles. En ningún caso se toma fotos o se accede a las fotos almacenadas en el dispositivo móvil.*
- *Referente a la funcionalidad del teléfono, como explicó en el punto anterior, es para el envío del mensaje de texto de confirmación y para las llamadas del servicio de atención de bienestar emocional. En ningún caso se accede a los datos de contactos telefónicos del Titular.*

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

Respuesta:

La información solicitada en los diferentes módulos o funcionalidades de la app y la interfaz web (el contenido es el mismo en ambas interfaces), obedece a lo mínimo requerido para gestionar: permiso de movilidad, citas médicas, brindar ayuda psicológica, mapear los sitios de mayor riesgo de contagio, informar a la ciudadanía sobre el comportamiento del virus, identificar a los infractores para informar a las autoridades competentes.
La descripción de los datos solicitados y su uso de manera detallada, se dio en la pregunta anterior.

(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:

Si se tuvo en cuenta lo preceptuado en el artículo 6 de la Ley 1581 de 2012, en concordancia con el artículo 6 del Decreto 1377 de 2013, respecto al tratamiento de datos sensibles, entendidos como aquellos que afectan directamente la intimidad de los mismos, dado que la recolección de tales datos personales, se hace previa autorización expresa por parte del Titular, cuando ingresa a la aplicación "ValleCorona", encuentra la casilla de verificación para aceptar las políticas de uso y privacidad, el enlace remite al apartado "instructivo de términos y condiciones de uso de la aplicación ", en cuanto a las políticas de privacidad, el enlace conduce al micro sitio donde se encuentran los siguientes documentos: política de seguridad de información de la Gobernación del Valle del Cauca, allí se informa el canal de atención, en el apartado "tratamiento de datos personales", es decir, cuando el ciudadano accede a la plataforma digital o aplicación "Vallecorona", y antes del acceso y su suso, debe dar click en una casilla donde se le informa que, de proseguir el uso de la aplicación, estaría aceptando de forma expresa los términos y condiciones y donde se especifican las finalidades del tratamiento, los datos que se recolectarán y las razones de dicho tratamiento."

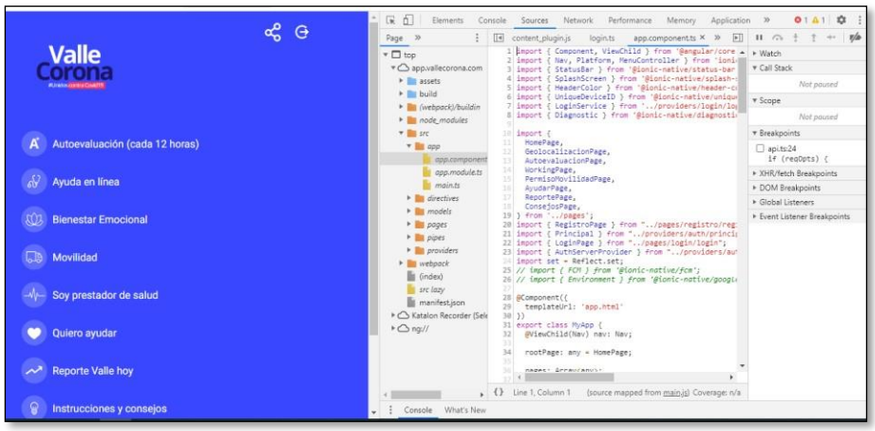
CUARTO: Que, de conformidad con la respuesta dada por el Secretario de las TIC de la Gobernación del Valle del Cauca, y en la medida que el Responsable del tratamiento de la información que sea recolectada en la aplicación "ValleCorona", es la Gobernación del Valle del Cauca, esta Dirección procedió a acumular los radicados 20-155788 y 20-155849,

QUINTO: Que frente al tratamiento de los datos personales realizado por la Gobernación del Valle del Cauca a través del aplicativo y página web denominada "ValleCorona" esta Dirección realizó un Análisis de Vulnerabilidades a la citada plataforma y aplicación cuyas recomendaciones y conclusiones fueron las siguientes:

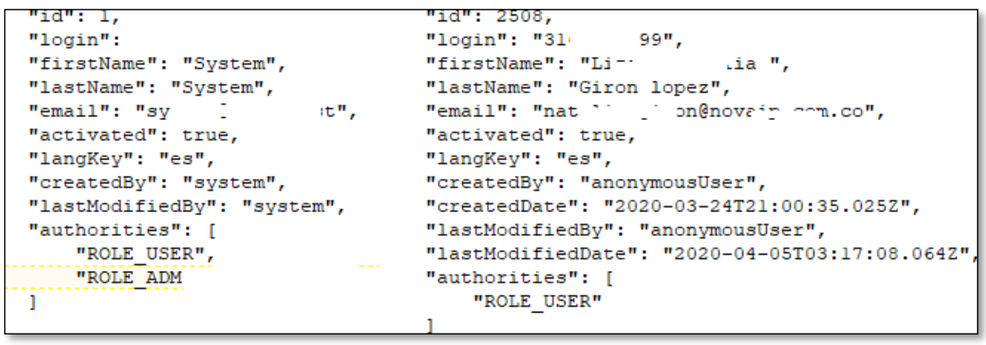
1. ***Realizar urgentemente la compilación de la aplicación y asegurar que no se muestre el código fuente para evitar que se publique información registrada en el sistema.***
2. *Depurar la información existente en la base de datos y borrar los datos que se utilizaron para las pruebas de la plataforma.*
3. *Implementar funcionalidad que permita actualizar datos o remover la información de un usuario registrado previamente.*
4. *Depurar los permisos solicitados por la aplicación y mantener únicamente los necesarios según la funcionalidad que se ofrece.*
5. *Se debe revisar la alerta de severidad "X-Frame-Options Header Not Set" encontrada en la página principal de la plataforma.*
6. *Los datos de síntomas quedan asociados a una línea celular y solo se permite este registro cada 12 horas; con este esquema no es claro cómo los ciudadanos pueden ingresar síntomas de personas mayores o menores de edad que no tengan línea celular independiente. Bajo este modelo la solución implementada no cumple a cabalidad con la finalidad de recolectar información y permitir ubicar focos de contagio.*
7. *Se deben implementar mecanismos que permitan garantizar que la información sea registrada por los titulares de esta para evitar registro de datos erróneos o fraudulentos.*

Ahora bien, respecto de lo señalado en el numeral 1 del citado Análisis de Vulnerabilidades determinó lo siguiente:

Revisión Plataforma
Dentro del proceso de revisión se evidenció que esta aplicación se encuentra implementada en Angular, pero no está compilada para ambiente productivo y por lo tanto es posible ver el código fuente, definir puntos de ruptura en la ejecución y cambiar valores de las variables para afectar su funcionamiento.



Debido a esta significativa falla de seguridad, fue posible deducir servicios expuestos por la aplicación y ejecutar los servicios "api/users", "api/empresa-sedes" y "api/empresas", los cuales arrojaron información relacionada con los usuarios y empresas registradas en esta plataforma.



Como puede observarse la conclusión descrita en el numeral 1 pone de presente que la plataforma "ValleCorona", presenta una vulnerabilidad en materia de seguridad, en la medida que es posible consultar el código fuente con el que fue configurada la página web por lo que podría accederse a la información recolectada.

A partir de lo anterior, esta Dirección procede a presentar las siguientes consideraciones:

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, ***"l****a 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 puedan 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.

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"***[4]

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

Los datos sensibles fueron definidos en la ley 1581 de 2012 y en el decreto 1377 de 2013[5] 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*"[6]. 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"*[7]

El artículo 10 de la Ley Estatutaria 1581 de 2012 permite el tratamiento de datos sin la autorización de las personas en los siguientes casos:

> *"(…) ARTÍCULO 10. CASOS EN QUE NO ES NECESARIA LA AUTORIZACIÓN. La autorización del Titular no será necesaria cuando se trate de:*
> ***a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;***
> *b) (..)*
> ***c) Casos de urgencia médica o sanitaria**;*
> *(…)*
> *Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley (...)". (Negrilla fuera del texto original).*[8]

Es importante resaltar que la recolección de datos sin autorización no significa que quede sin protección esa información y los ciudadanos titulares de los datos. En efecto, la parte final de esa norma señala que "*quien acceda a los datos personales sin que medie autorización previa* ***deberá en todo caso cumplir con las disposiciones contenidas en la presente ley***". (Destacamos) La autorización es un mecanismo de legitimación para tratar datos personales, pero no una forma de protección de los derechos. La efectiva protección de los derechos dependerá de las medidas que implementen los Responsables del tratamiento para garantizar el uso debido de los datos, su seguridad, confidencialidad, etc.

Nótese que la regulación sobre tratamiento de datos exige que las personas sean debidamente informadas sobre ciertos aspectos. En este sentido, el artículo 6 del decreto 1377 de 2013 (incorporado en el artículo 2.2.2.25.2.3 decreto 1074 de 2015) ordena lo siguiente:

> *"**ARTÍCULO 2.2.2.25.2.3. DE LA AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES SENSIBLES.** El Tratamiento de los datos sensibles a que se refiere el artículo 5o de la Ley 1581 de 2012 está prohibido, a excepción de los casos expresamente señalados en el artículo 6o[9] de la citada ley.*

---

[5] Norma compilada en el Decreto Único Reglamentario 1074 de 2015.
[6] Artículo 5 de la ley 1581 de 2012, repetido en el numeral 3 del artículo 3 del decreto 1377 de 2013
[7] Cfr. Corte Constitucional, sentencia C-748 de 2011, numeral 2.7.3
[8] Como es sabido, la Corte Constitucional declaró exequible el artículo 10 sin que formulara alguna interpretación o condicionamiento sobre dichas disposiciones, como lo hizo para el caso del artículo 8. En efecto, respecto del artículo 8 de la Ley 1581 de 2012 la Corte Constitucional resolvió lo siguiente: "*Cuarto.- Declarar EXEQUIBLE el artículo 8 del proyecto de ley objeto de revisión, excepto la expresión "sólo", del literal e) que se declara INEXEQUIBLE. De la misma manera, el literal e) debe entenderse en el sentido que el Titular también podrá revocar la autorización y solicitar la supresión del dato, cuando no exista un deber legal o contractual que le imponga el deber de permanecer en la referida base de datos."* Todo lo anterior se puede constatar en los numerales segundo y cuarto de la parte resolutiva de la sentencia C-748 de 2011 de dicha Corte.
[9] **ARTÍCULO 6o. TRATAMIENTO DE DATOS SENSIBLES.** Se prohíbe el Tratamiento de datos sensibles, excepto cuando:
a) El Titular haya dado su autorización explícita a dicho Tratamiento**, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;**
b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización;
c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran

> *En el Tratamiento de datos personales sensibles, cuando dicho Tratamiento sea posible conforme a lo establecido en el artículo 6o 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)

Mediante la plataforma "ValleCorona" se recolectan datos sensibles relacionados con el estado de salud de las personas y sus posibles síntomas. Si bien no es obligatorio que el ciudadano suministre su información sensible, tampoco se le informa cuáles de los datos solicitados son sensibles. En otras palabras, el ciudadano suministraría información si saber que es de naturaleza sensible y que es facultativo suministrar esa clase de datos.

En el aparte de CONDICIONES DE USO – Objeto del documento Instructivo de Términos y Condiciones de la Plataforma "ValleCorona", se estableció lo siguiente:

> *"Estos términos y condiciones regulan la forma de emplear y usar la aplicación ValleCorona, el usuario podrá realizar cualquier colaboración, acceso o descarga de la información suministrada en esta aplicación. Al acceder o utilizar ValleCorona usted acepta plenamente, sin reservas y está de acuerdo en cumplir con estos términos y condiciones de uso, denominados en adelante para este documento "Términos y Condiciones". Estos Términos y Condiciones consisten en un acuerdo colaborativo entre usted y ValleCorona, que abarca todo su acceso y uso, lo que incluye el uso de toda la información, datos, herramientas, productos, servicios y otro contenido disponible mediante la aplicación.* ***En caso de no estar de acuerdo con estos Términos y Condiciones le sugerimos que se abstenga de usar ValleCorona. Al utilizar esta aplicación, usted confirma que comprende y está de acuerdo con las siguientes condiciones****…" (Negrilla fuera de texto)*

La anterior cláusula, carece de los requisitos establecidos en el numeral 2 del citado artículo 6 del Decreto 1377 de 2013 (incorporado en el Decreto 1074 de 2015), en el sentido que, no le informa al ciudadano de manera explícita y previa lo siguiente: (i) los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal; (ii) qué datos objeto de recolección y de tratamiento son de carácter sensible.

Téngase presente que los ciudadanos no son expertos en regulación de tratamiento de datos. Tampoco se puede asumir que todas las personas sepan que son datos sensibles ni cual información que se le solicita es de dicha categoría. Por eso, se les debe comunicar ese aspecto de manera clara y sencilla para que ellos tomen una decisión suficientemente informada.

Así las cosas, se le impartirá una orden a la Gobernación del Valle del Cauca con el fin de que adecue el documento "Instructivo de Términos y Condiciones de la Plataforma ValleCorona" en lo relacionado con el tratamiento de datos personales sensibles, para que informe de manera clara y sencilla todo lo que exige la regulación para su tratamiento.

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

---

exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular;
d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;
e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

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*"[10].

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 26[11] -*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 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*[12]*(accountability)*[13]".

El término "*accountability"*[14], 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.

---

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

[11] 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 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"*

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

[13] *"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.

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

Conforme con ese análisis, las recomendaciones que trae la guía frente al cumplimiento de la Ley 1581 de 2012, por parte de los obligados 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 naturaleza[15] para garantizar el correcto cumplimiento de los deberes que imponen las regulaciones sobre Tratamiento de Datos Personales. El mismo, exige que los Responsables del Tratamiento adopten medidas apropiadas, efectivas y verificables que le permitan evidenciar la observancia de las normas sobre la materia.

Dichas acciones o medidas, deben ser objeto de revisión y evaluación permanente para medir su nivel de eficacia y el grado de protección de los Datos personales.

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

Adicionalmente, el reto de las organizaciones frente al Principio de Responsabilidad Demostrada va mucho más allá de la mera expedición de documentos o redacción de políticas. Como se ha manifestado, exige que se demuestre el cumplimiento real y efectivo en la práctica de sus funciones.

En este sentido, desde el año 2006 la Red Iberoamericana de Protección de Datos (RIPD) ha puesto de presente que, "*la autorregulación sólo* [sic] *redundará en beneficio real de las personas en la medida que sea bien concebida, aplicada y cuente con mecanismos que garanticen su cumplimiento de manera que* ***no se constituyan en meras declaraciones 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****"*[16].(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.

---

[15] 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.

[16] 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.

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*"[17] 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*"[18].

CONCLUSIONES:

1. La Gobernación del Valle del Cauca es el Responsable del tratamiento de los datos que se recolectan a través de la plataforma y la App "CoronaValle"

2. A junio 25 de 2020 se encuentran 69.332 personas registradas en la base de datos de "ValleCorona".

3. En el análisis de vulnerabilidades realizado por esta Dirección se encontró que la plataforma "ValleCorona", presenta una vulnerabilidad en materia de seguridad, en la medida que es posible consultar el código fuente con el que fue configurada la página web por lo que podría accederse a la información recolectada.

4. Mediante la plataforma "ValleCorona", se solicita información relacionada al estado de salud de las personas, la cual es considerada como datos sensibles, según el artículo 5 de la Ley Estatutaria 1581 de 2012, por lo que es necesario que se adecúe el Instructivo de Términos de Condiciones para el uso de la citada plataforma, en lo relacionado con el tratamiento de los datos personales sensibles.

Así las cosas, esta Dirección impartirá órdenes administrativas, para que, la Gobernación del Valle del Cauca en su calidad de Responsable del tratamiento de los datos personales recolectados o tratados en la plataforma "ValleCorona", (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 (3) Adecúe El Instructivo de Términos y Condiciones de Uso de la plataforma "ValleCorona", en lo relacionado con el tratamiento de datos sensibles.

En mérito de lo expuesto, este Despacho

RESUELVE

ARTÍCULO PRIMERO: ORDENAR a la **GOBERNACIÓN DEL VALLE DEL CAUCA**, identificada con el NIT. 890.399.029-5 que implemente medidas de seguridad apropiadas y efectivas para impedir que personas no autorizadas accedan o descarguen la información recolectada y tratada a través de plataforma "ValleCorona", de conformidad con lo establecido en la parte considerativa del presente acto administrativo. Dichas medidas deben ir acompañadas de mecanismos de monitoreo y control que de manera permanente permitan asegurar la debida protección de la información tratada.

ARTÍCULO SEGUNDO: ORDENAR a la **GOBERNACIÓN DEL VALLE DEL CAUCA**, identificada con el NIT. 890.399.029-5 que modifique el documento "Instructivo de Términos

[17] Cfr. Superintendencia de Industria y Comercio (2015) "*Guía para implementación del principio de responsabilidad demostrada (accountability)*", págs 16-18.
[18] *Ibidem*.

y Condiciones para el uso de la plataforma y aplicativo “ValleCorona”, de manera que informe todo lo que ordena la regulación colombiana respecto del tratamiento de datos sensibles, en particular el artículo 6 del decreto 1377 de 2013 (incorporado en el artículo 2.2.2.25.2.3 decreto 1074 de 2015) en concordancia con el artículo 12 de la Ley Estatutaria 1581 de 2012, a saber: a) Cuáles de los datos solicitados son de naturaleza sensible; b) Que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento; c*)* Que es facultativo responder las preguntas sobre datos sensibles;

ARTÍCULO TERCERO: ORDENAR a la **GOBERNACIÓN DEL VALLE DEL CAUCA**, identificada con el NIT. 890.399.029-5 que fortalezca las medidas adoptadas respecto del tratamiento de datos sensibles de manera que esa información tenga mayores medidas de seguridad y restricciones de acceso, uso o circulación, de tal forma que no sólo se implemente la “responsabilidad demostrada”[19] sino la “*responsabilidad reforzada”*, la cual, 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 CUARTO: La **GOBERNACIÓN DEL VALLE DEL CAUCA**, identificada con el NIT. 890.399.029-5 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 Gobernadora del Valle del Cauca mediante la cual acrediten que se han implementado las medidas ordenadas.

ARTÍCULO QUINTO: Notificar el contenido de la presente resolución a la **GOBERNACIÓN DEL VALLE DEL CAUCA** 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., 18 AGOSTO 2020

EL DIRECTOR DE INVESTIGACIÓN DE PROTECCIÓN DE DATOS PERSONALES,

CARLOS ENRIQUE SALAZAR MUÑOZ
Firmado digitalmente por CARLOS ENRIQUE SALAZAR MUÑOZ
Fecha: 2020.08.18 16:54:18 -05'00'

CARLOS ENRIQUE SALAZAR MUÑOZ

Proyectó: JATS
Revisó: NTL
Aprobó: CESM

[19] Cfr. Artículos 26 y 27 del Decreto 1377 de 2013 (Incorporado en el Decreto 1074 de 2015)

NOTIFICACIÓN:

Entidad: **GOBERNACIÓN DEL VALLE DE CAUCA**
Identificación: Nit. 890.399.029-5
Representante legal: **CLARA LUZ ROLDÁN GONZÁLEZ**
Identificación: C.C. 51.649.242
Ciudad: Cali – Valle del Cauca
Correo electrónico: njudiciales@valledelcauca.gov.co
contactenos@valledelcauca.gov.co