

REPÚBLICA DE COLOMBIA



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

RESOLUCIÓN NÚMERO 39508 DE 2021

(28 JUNIO DE 2021)

“Por la cual se impone una sanción”

VERSIÓN ÚNICA

Radicación 20-221040

EL DIRECTOR DE INVESTIGACIÓN DE PROTECCIÓN 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 los numerales 5 y 9 del artículo 17 del Decreto 4886 de 2011 y

CONSIDERANDO

PRIMERO: Que mediante oficio radicado bajo el número 20-221040-1 de fecha 8 de julio de 2020 este Despacho requirió a la Presidente Ejecutiva de la **CÁMARA DE COMERCIO DE MONTERÍA**, identificada con el Nit. 891.080.019-4, (en adelante **CÁMARA DE COMERCIO**), para que informara lo siguiente:

1. *¿La recolección y Tratamiento de los Datos la realizan directamente la Cámara de Comercio de Montería 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 ese tipo de información?*

En caso de que acuda a los servicios de un tercero, por favor adjuntar el contrato correspondiente.

2. *¿Antes de diseñar la página web 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)? De ser así, por favor remitirlo.*
3. *¿Se realizó una evaluación de los riesgos específicos para los derechos y libertades de los Titulares de los Datos personales? Si así fue, deberá, anexar el respectivo documento que lo acredite.*
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 expuestas las personas como consecuencia del Tratamiento de su información a través de la página web de esa organización?. En caso de que la respuesta a este interrogante sea positiva, por favor enviar la evidencia correspondiente.*
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 su página web?*
6. *Qué medidas tecnológicas; humanas; administrativas; físicas; contractuales; entre otras, ha implementado la Cámara de Comercio de Montería, con el fin de evitar lo siguiente respecto del manejo de la información:*
 - i. *Accesos y/o usos indebidos o no autorizados;*
 - ii. *Manipulación;*
 - iii. *Destrucción;*
 - iv. *Circulación o suministro de la de los Datos a personas no autorizadas.*
7. *¿Esas medidas de seguridad son objeto de revisión, evaluación y mejora permanente?*
8. *¿Se han presentado incidentes de seguridad? De ser así, por favor informe ¿cuántos reclamos se han presentado y cuál fue la gestión adelantada frente a esto?*
9. *¿Con cuáles empresas; plataformas digitales; y/o entidades se realiza intercambio o envió de Datos de los Titulares? Y ¿por qué causa?.*
10. *¿Dónde están almacenadas, y cómo se obtienen las Autorizaciones de los Titulares para el Tratamiento sus Datos por parte de terceros?*
11. *De ser el caso, ¿cuál es la información que se comparte y/o transmite? Por favor especificar.*
12. *¿Cuál es el Tratamiento que aplica cada tercero a los Datos recolectados?*
13. *De conformidad con lo establecido en el artículo 11 del Decreto 1377 de 2013 (compilado en el Decreto 1074 de 2015), y en atención a las limitaciones temporales en el Tratamiento de Datos personales, ¿Cuál ha sido el*

- procedimiento establecido por esa organización para suprimir la información que se recolecte mediante su sitio web?
14. De conformidad con lo establecido en el artículo 4 del Decreto 1377 de 2013 (compilado en el Decreto 1074 de 2015) ¿qué procedimientos se establecieron para determinar que la información solicitada en la página web, es pertinente y adecuada para la finalidad del registro?
15. Así pues, por favor explique, ¿Por qué razón cada uno de los Datos recolectados son indispensables para cumplir la finalidad informada?
16. Finalmente, teniendo en cuenta los procedimientos fijados informe si, ¿se tuvo en cuenta lo dispuesto por 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”.

SEGUNDO: Que mediante Oficio radicado con el número 20-221040-3 de fecha 15 de julio de 2020, la Presidente Ejecutiva (e) de la **CÁMARA DE COMERCIO** dio respuesta al citado requerimiento en los siguientes términos:

1. ¿La recolección y Tratamiento de los Datos la realizan directamente la Cámara de Comercio de Montería 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 ese tipo de información?

R/: Entendiendo ‘Tratamiento’, de conformidad la definición prevista por el literal g), artículo 3° de la Ley 1581 de 2012, como cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. De acuerdo con lo establecido por el literal d), artículo 3° de la Ley 1581 de 2012, la calidad de Encargado del Tratamiento se adquiere cuando una persona natural o jurídica, pública o privada, por sí misma o en asocio con otros, realiza el tratamiento de datos personales por cuenta del responsable del tratamiento, haciéndose exigibles una serie de deberes consagrados en el artículo 18 de la misma Ley.

En este marco, Confecámaras cumple el papel de encargado del tratamiento de la información pública del SII, RUES, RNT y RUNEOL, contenida en las plataformas tecnológicas administrada por la Confederación, por mandato de las Cámaras de Comercio.

Por su parte, la Cámara de Comercio de Montería en su página web, realiza la recolección y Tratamiento de los Datos personales directamente.

2. ¿Antes de diseñar la página web 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)? De ser así, por favor remitirlo.

R/: En relación con la información pública del SII, RUES, RNT y RUNEOL, contenida en las plataformas tecnológicas administrada por la Confederación en calidad de ‘Encargado’, Confecamaras en su proceso de implantación de un sistema de gestión de seguridad de la información basado en ISO 27001 ha adoptado el cumplimiento del control 18.1.4 de ISO 27001 cuyos estudios están en análisis de riesgos de la Confederación.

En relación con la naturaleza de la información contenida en estas bases de datos en donde la Confederación cumple el rol de ‘Encargado del Tratamiento’, se determinó que todos los datos allí contenidos tienen naturaleza pública.

La función registral tiene un carácter eminentemente público y en consecuencia, toda la información allí consignada comparte la misma naturaleza. Esta particularidad permite que cualquier persona pueda tener acceso a los datos allí inscritos a través de diversos mecanismos desarrollados por las Cámaras para facilitar su acceso, ya que, la principal función que cumple el registro público que llevan las Cámaras de Comercio, es la de otorgar publicidad de los actos y documentos registrales y su consecuente oponibilidad frente a terceros, según lo establecido en el artículo 29, numeral 4 del Código de Comercio. En concordancia con lo anterior, el artículo 2.2.2.25.1.3., del Decreto 1074 de 2015, señala la siguiente definición de dato público:

“Dato público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva”.

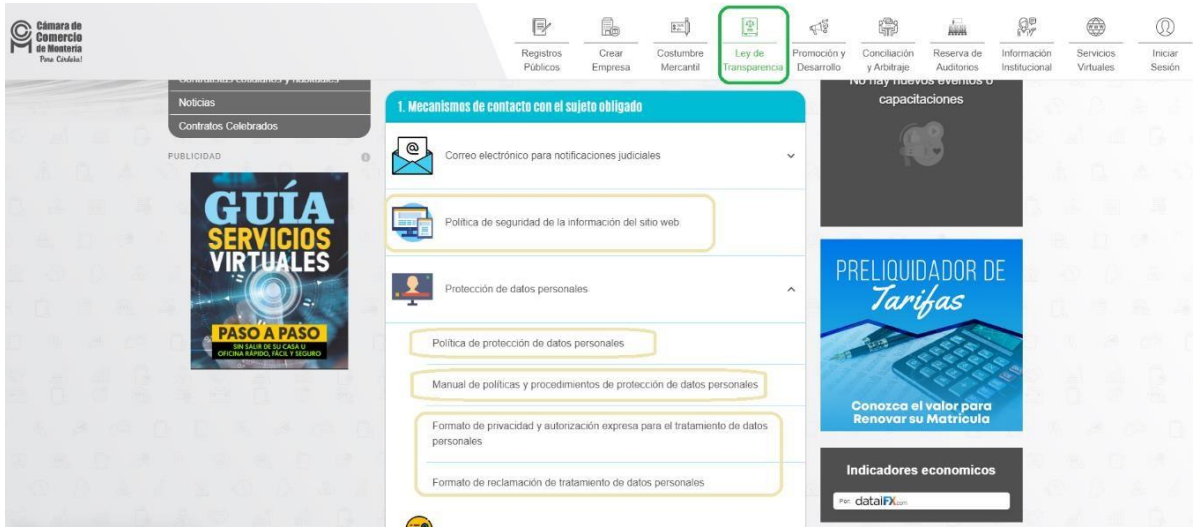
La Cámara de Comercio de Montería en su página web no aplicó dicho estudio de impacto de privacidad.

3. ¿Se realizó una evaluación de los riesgos específicos para los derechos y libertades de los Titulares de los Datos personales? Si así fue, deberá, anexo el respectivo documento que lo acredite.

R/: En relación con la información pública del SII, RUES, RNT y RUNEOL, contenida en las plataformas tecnológicas administrada por la Confederación en calidad de ‘Encargado’, se han identificado y controlado riesgos orientados a la confidencialidad de la información en dichas bases de datos.

La Cámara de Comercio de Montería, no hizo una evaluación de los riesgos específicos para los derechos y libertades de los Titulares de los Datos personales, sin embargo, si cuenta con unas Políticas,

procedimientos y formatos de protección de datos personales que permiten evitar que se materializasen los posibles riesgos a que haya lugar, documentos que se pueden encontrar en nuestra pagina web en la sección de ley de transparencia como se indica en la imagen.



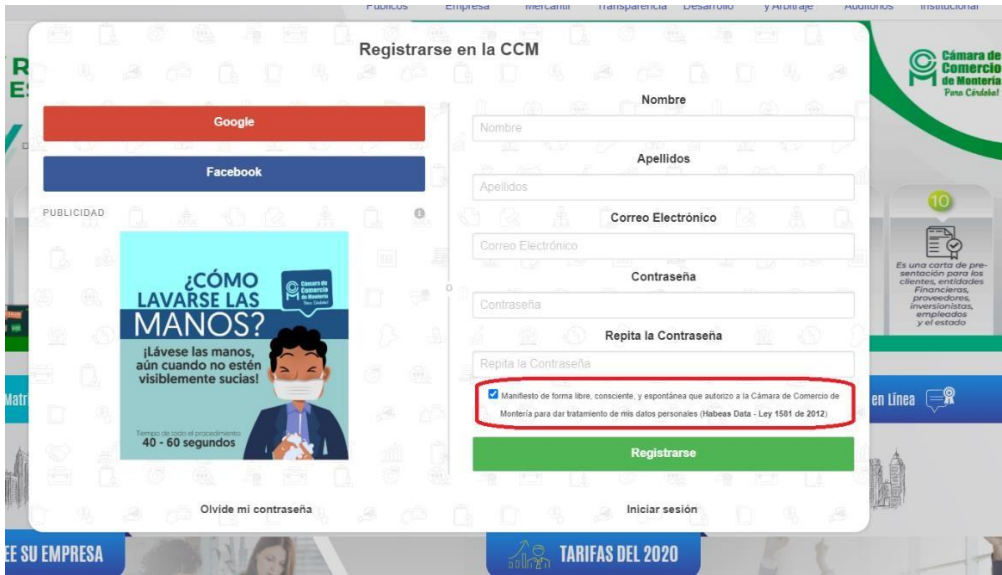
4. ¿Se desarrolló y puso en marcha un sistema de administración de riesgos asociados al Tratamiento de Datos personales que les permita identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestas las personas como consecuencia del Tratamiento de su información a través de la página web de esa organización? En caso de que la respuesta a este interrogante sea positiva, por favor enviar la evidencia correspondiente.

R/: En Cámara de Comercio de Montería no se ha desarrollado el sistema de administración de riesgos asociados al tratamiento de datos personales, sin embargo, se trata de minimizar los riesgos a través de acciones como el diseño e implementación de políticas de seguridad de tratamiento de datos personales.

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 su página web?

R/: Desde la Confederación a las Cámaras de Comercio se les facilita la creación de alertas y documentos base como la política de tratamiento de datos personales y privacidad, dando cumplimiento a lo requerido por la Ley 1581 de 2012.

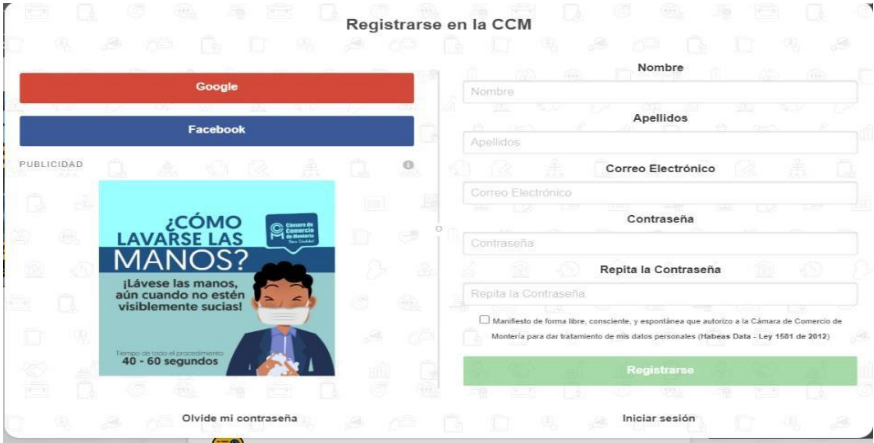
La Cámara de Comercio de Montería en su página web establece mecanismos a través de los cuales las personas manifiestan su aprobación para el adecuado uso del tratamiento de los datos personales que aquí se reporten, como se evidencia en la siguiente imagen.



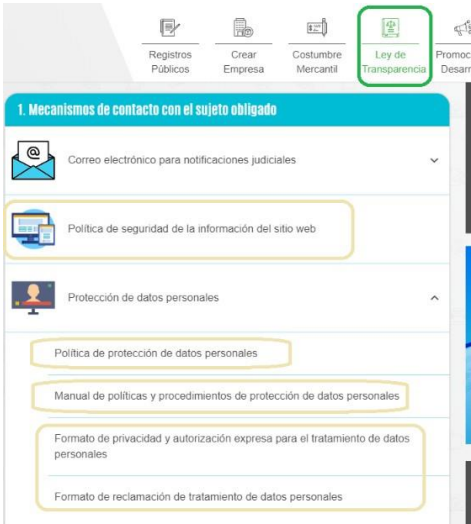
6. Qué medidas tecnológicas; humanas; administrativas; físicas; contractuales; entre otras, ha implementado la Cámara de Comercio de Montería, con el fin de evitar lo siguiente respecto del manejo de la información:

- i. Accesos y/o usos indebidos o no autorizados
- ii. Manipulación
- iii. Destrucción
- iv. Circulación o suministro de la de los Datos a personas no autorizadas.

R/: La Cámara de Comercio de Montería ha implementado para la parte de accesos y/o usos indebidos o no autorizados un sistema de registro donde la persona crea un usuario y contraseña el cual es único e intransferible en donde el usuario final otorga o no el permiso de tratamiento de datos personales como lo muestra la imagen de creación de usuario.



Al mismo tiempo la manipulación y destrucción del tratamiento de datos personales además de que la persona autoriza el tratamiento de datos personales como se muestra en la imagen anterior, si esta quisiera hacer un reclamo o destrucción, en nuestra sección de ley de transparencia tenemos publicados los documentos adecuados para esta gestión y como cámara poder proceder a la solicitud. Ver siguiente imagen.



7. ¿Esas medidas de seguridad son objeto de revisión, evaluación y mejora permanente?
- R/:** Las políticas y procedimientos de protección de datos personales de la Cámara de Comercio de Montería, permiten que se analicen de manera constante y que se ajusten de acuerdo con la necesidad y en busca de la mejora continua.
8. ¿Se han presentado incidentes de seguridad? De ser así, por favor informe ¿cuántos reclamos se han presentado y cuál fue la gestión adelantada frente a esto?
- R/:** La Cámara de comercio de Montería conoce de incidentes de seguridad reportados a otras autoridades competentes, por lo tanto, no tenemos conocimiento exacto del número de casos presentados.
- Para tratar esta problemática hemos puesto en conocimiento a confecamaras a fin de que en lo pertinente se analice estos incidentes, así como, también se ha llevado a cabo reuniones con dichas autoridades con el fin de buscar posibles soluciones que permitan disminuir este tipo de incidentes reportados.
9. ¿Con cuáles empresas; plataformas digitales; y/o entidades se realiza intercambio o envió de Datos de los Titulares? Y ¿por qué causa?
- R/:** La Cámara de comercio de Montería suministra los datos de los titulares a Confecamaras, ya que es el 'Encargado del tratamiento de datos'.
10. ¿Dónde están almacenadas, y cómo se obtienen las Autorizaciones de los Titulares para el Tratamiento sus Datos por parte de terceros?
- R/:** En relación con la información pública del SII, RUES, RNT y RUNEOL, contenida en las plataformas tecnológicas administrada por la Confederación en calidad de 'Encargado', es necesario advertir que todos los datos allí contenidos tienen la naturaleza de 'Dato Público', en tal sentido, de conformidad con lo establecido por el artículo 10° de la Ley 1581 de 2012, no es necesaria la autorización del titular para el tratamiento de sus datos.

“Artículo 10. Casos en que no es necesaria la autorización. La autorización del Titular no será necesaria cuando se trate de:

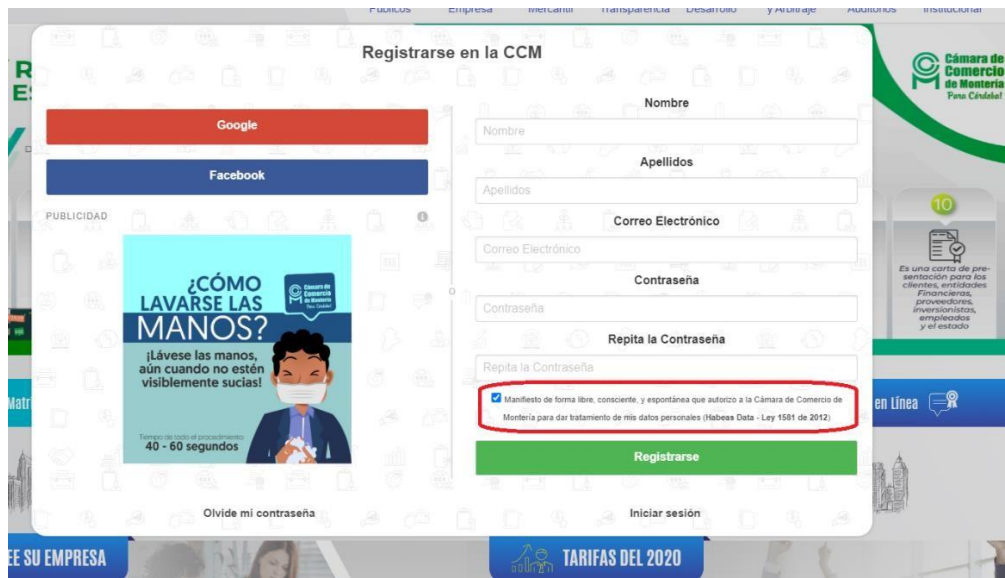
Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;
Datos de naturaleza pública;

Casos de urgencia médica o sanitaria;
Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;
Datos relacionados con el Registro Civil de las Personas.

Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley”.

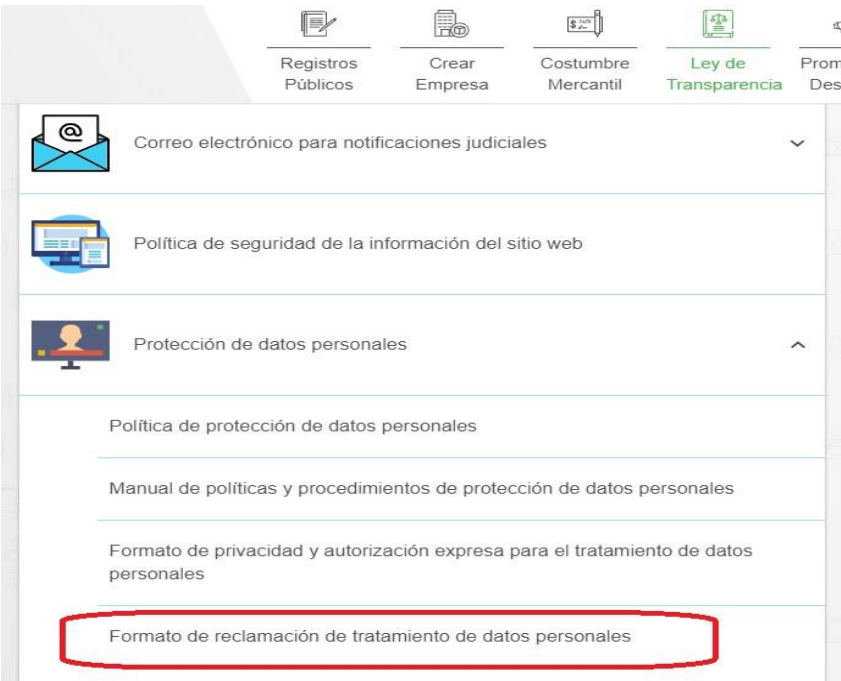
La información contenida en los registros públicos como es el caso del Registro Mercantil es considerada como dato público, por definición legal es de carácter público Artículo 26 Código de Comercio. Los datos públicos son aquellos que por mandato legal o constitucional son calificados como tal y los que no tengan la naturaleza de semiprivado, privado o sensible, a dichos datos podrá accederse sin autorización del titular.

La Cámara de Comercio de Montería en su página web establece mecanismos a través de los cuales las personas manifiestan su aprobación para el adecuado uso del tratamiento de los datos personales que aquí se reporten, como se evidencia en la siguiente imagen.



11. De ser el caso, ¿cuál es la información que se comparte y/o transmite? Por favor especificar.
- R/: La Cámara de Comercio de Montería comparte y/o transmite la información recolectada en los registros públicos. (Nombre, Dirección, teléfono, correo, identificación, teléfono o celular, actividad económica, etc)
12. ¿Cuál es el Tratamiento que aplica cada tercero a los Datos recolectados?
- R/: Confecamaras se encarga de almacenar y publicar esta información de los terceros en las distintas plataformas tecnológicas asociadas el RUES como los son SII, RNT, RONEOL.
13. De conformidad con lo establecido en el artículo 11 del Decreto 1377 de 2013 (compilado en el Decreto 1074 de 2015), y en atención a las limitaciones temporales en el Tratamiento de Datos personales, ¿Cuál ha sido el procedimiento establecido por esa organización para suprimir la información que se recolecte mediante su sitio web?
- R/: De conformidad con lo establecido por el artículo 11 del Decreto 1377 de 2013:
En relación con la información pública del SII, RUES, RNT y RONEOL, contenida en las plataformas tecnológicas administrada por la Confederación en calidad de ‘Encargado’, es de advertir que si bien el titular de datos personales, tiene el derecho en todo momento, a solicitar a la Cámara de Comercio la supresión de sus datos personales, cuando se trata de datos contenidos en las bases de datos de los registros públicos, la Cámara de Comercio tiene la obligación de mantenerlos como públicos y a almacenarlos en las condiciones y términos establecidos en las normas legales y reglamentarias.

La Cámara de comercio de Montería en su pagina web tiene estipulado un formato de supresión o formato de reclamación de tratamiento de datos personales en la sección o link de ley de transparencia como se muestra en la imagen.



14. De conformidad con lo establecido en el artículo 4 del Decreto 1377 de 2013 (compilado en el Decreto 1074 de 2015) ¿qué procedimientos se establecieron para determinar que la información solicitada en la página web, es pertinente y adecuada para la finalidad del registro?

R/: En relación con la información pública del SII, RUES, RNT y RONEOL, contenida en las plataformas tecnológicas administrada por la Confederación en calidad de ‘Encargado’, es de precisar que la función registral tiene un carácter eminentemente público y en consecuencia, toda la información allí consignada comparte la misma naturaleza. Esta particularidad permite que cualquier persona pueda tener acceso a los datos allí inscritos a través de diversos mecanismos desarrollados por las Cámaras para facilitar su acceso, ya que, la principal función que cumple el registro público que llevan las Cámaras de Comercio, es la de otorgar publicidad de los actos y documentos registrales y su consecuente oponibilidad frente a terceros.

Desde el proceso de promoción y desarrollo se crean eventos en la página web que requieren el registro de aquellos terceros que van a participar, para lo cual se establecieron unos datos que se consideran pertinentes y adecuados, ya que a través de estos eventos se emiten certificaciones que requieren de datos básicos para la generación del mismo.

15. Así pues, por favor explique, ¿Por qué razón cada uno de los Datos recolectados son indispensables para cumplir la finalidad informada?

R/: Como se dijo anteriormente, de estos registros se expiden certificaciones de asistencia, homologando tiempo “duración en horas”, tipo identificación, nombre, número de identidad y correo electrónico con el fin de hacer el envío de esta certificación vía email.

16. Finalmente, teniendo en cuenta los procedimientos fijados informe si, ¿se tuvo en cuenta lo dispuesto por 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”.

R/: En relación con la información pública del SII, RUES, RNT y RONEOL, contenida en las plataformas tecnológicas administrada por la Confederación en calidad de ‘Encargado’, es necesario advertir que los datos contenidos en los registros públicos provienen del cumplimiento de una función reglada, cuyos formularios y procedimientos son autorizados por la Superintendencia de Industria y Comercio, y cumplen una finalidad de publicidad y oponibilidad.

Por lo tanto, en las bases de datos de los registros públicos sólo se recolecta la información y datos que expresamente la Ley y las normas reglamentarias han autorizado, se entiende que estos datos son de carácter público por disposición legal y dentro de ellos no se incluye ningún dato considerado como ‘sensible’ al tenor de la definición establecida por el artículo 5° de la Ley 1581 de 2012.

Por su parte la Cámara de comercio de Montería en su página web permite que las personas se inscriban a los eventos sin estar previamente registrado en el portal. Esto indica que si el usuario no acepta las políticas de tratamiento de datos personales al momento de inscribirse en el evento ofertado por el área de promoción y desarrollo, de igual forma podrá participar sin ningún inconveniente.

TERCERO: Que el Grupo de Trabajo de Informática Forense y Seguridad Digital de esta Superintendencia, realizó la preservación de la página web de la **CÁMARA DE COMERCIO** (www.ccmonteria.org), relacionando en el Acta No. 068 del 17 de julio de 2020, los hallazgos encontrados sobre la protección de datos personales.

CUARTO: Que mediante Resolución 51634 del 28 de agosto de 2020, este Despacho resolvió formular pliego de cargos contra la **CÁMARA DE COMERCIO**, como se indica a continuación:

*“**ARTÍCULO PRIMERO. FORMULAR PLIEGO DE CARGOS** contra la Cámara de Comercio de Montería identificada con el Nit. 891080019, por la presunta vulneración del deber de solicitar la Autorización al Titular para el Tratamiento de sus Datos personales, contenido en el literal b) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal c) del artículo 4 y el artículo 9 de la misma ley. Así como del artículo 5 del Decreto 1377 de 2013 (incorporado en el artículo 2.2.2.25.2.2 del Decreto 1074 de 2015) de conformidad con lo señalado anteriormente y resumido en la Tabla número uno, titulada “Relación de presuntos incumplimientos de la Cámara de Comercio de Montería respecto del Tratamiento de Datos que realiza mediante formularios que utiliza en su página web.”*

***ARTÍCULO SEGUNDO. FORMULAR PLIEGO DE CARGOS** contra la Cámara de Comercio de Montería identificada con el Nit. 891080019 por el presunto incumplimiento del deber de informar al Titular al momento de solicitar la Autorización lo establecido en los literales a); b); c); y d) del artículo 12 de la Ley 1581 de 2012, en concordancia con los literales b); c) y e) del artículo 8 de la misma norma.*

***ARTÍCULO TERCERO. FORMULAR PLIEGO DE CARGOS** contra la Cámara de Comercio de Montería identificada con el Nit. 891080019 por la presunta violación del deber de informar al Titular sobre las finalidades del Tratamiento al que serán sometidos sus Datos personales, de conformidad con lo establecido en el literal c) del artículo 17 en concordancia con el literal b) del artículo 4, el artículo 12 de la Ley 1581 de 2012, así como el inciso primero del artículo 2.2.2.25.2.2 del Decreto Único Reglamentario 1074 de 2015, de conformidad con la Tabla número uno, titulada “Relación de presuntos incumplimientos de la Cámara de Comercio de Montería respecto del Tratamiento de Datos que realiza mediante formularios que utiliza en su página web”.*

QUINTO: Que la Resolución 51634 del 28 de agosto de 2020 fue notificada de forma electrónica a la **CÁMARA DE COMERCIO** el mismo día, según consta en la certificación expedida por la Coordinadora del Grupo de Notificaciones y Certificaciones de esta Superintendencia, radicada bajo el número 20-221040-9 de fecha 25 de septiembre de 2020.

SEXTO: Que mediante oficio radicado en el sistema de trámites de la entidad bajo el número 20-221040-8 de fecha 16 de septiembre de 2020, el Presidente Ejecutivo de la **CAMARA DE COMERCIO** encontrándose dentro del término establecido para el efecto, a través de su apoderado presentó los respectivos descargos en los cuales manifestó, lo siguiente:

Consideraciones:

El artículo 15 de la Constitución Política establece que las personas, en desarrollo de sus derechos a la autodeterminación informática y el principio de libertad, son quienes de forma expresa deben autorizar que la información que sobre ellos sea recaudada pueda ser incluida en una base datos. Al respecto la Corte Constitucional ha señalado lo siguiente: “Principio de libertad: El tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

Este principio, pilar fundamental de la administración de datos, permite al ciudadano elegir voluntariamente si su información personal puede ser utilizada o no en bases de datos. También impide que la información ya registrada de un usuario, la cual ha sido obtenida con su consentimiento, pueda pasar a otro organismo que la utilice con fines distintos para los que fue autorizado inicialmente.

El literal c) del Proyecto de Ley Estatutaria no sólo desarrolla el objeto fundamental de la protección del habeas data, sino que se encuentra en íntima relación con otros derechos, el de intimidad y el libre desarrollo de la personalidad. En efecto, el ser humano puede determinar qué datos quiere sean conocidos.

Los principios rectores, además, deben confluir en cuanto a su aplicación contenidos en la Ley 1581 de 2012, específicamente en el presente caso los deberes que tienen los responsables de garantizar al titular, en todo ejercicio del derecho de hábeas data.

Igualmente, es importante indicar que, en virtud del principio de libertad, citado en líneas atrás, el legislador impuso a los responsables del Tratamiento de datos personales, la exigencia de requerir la autorización previa expresa e informada del Titular, consagrada en el artículo 9 de la Ley 1581 de 2012 y, además, el deber de solicitar y conservar copia de la autorización de Tratamiento otorgada por el mismo, dispuesto en el literal b) del artículo 17 del mismo compendio normativo.

Sumado a lo anterior, el mismo responsable debe conservar una copia de la autorización otorgada por el Titular de la información de forma tal que, en el momento en que sea solicitada para consulta, cuente con la misma.

De otra parte, es necesario mencionar que junto con el principio de libertad contiene el principio de finalidad el cual expresamente señala:

“Artículo 4°. Principios Para el Tratamiento de Datos Personales. En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:

(...)b) Principio de finalidad: El Tratamiento debe obedecer a una finalidad le Constitución y la Ley, la cual debe ser informada al Titular”.

De esta manera la mencionada norma estatutaria indicó en su artículo unos requisitos mínimos que deben ser informados al Titular al momento del Tratamiento de sus datos personales, el cual reza lo siguiente:

«ARTICULO 12. DEBER DE INFORMAR AL TITULAR. EL RESPONSABLE DEL TRATAMIENT AL MOMENTO DE SOLICITAR AL TITULAR LA AUTORIZACIÓN, DEBERÁ INFORMARLE DE MANERA CLARA Y EXPRESA LO SIGUIENTE:

- a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo.
- b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes.
- c) Los derechos que le asisten como Titular.
- d) La identificación, dirección física o electrónica y teléfono del responsable del Tratamiento.

De otra parte, se debe traer a colación que se entiende por dato sensible y cuando puede llegar a considerarse un dato biométrico como tal, al respecto es pertinente traer a colación el artículo 5 de la Ley 1581 de 2012 que definió los datos sensibles así: “se entiende por datos sensibles 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 (a salud, a la vida sexual y los datos biométricos”.

Así mismo, la Corte Constitucional mediante la sentencia C-1 011 de 2008 señaló respecto a los datos sensibles que “(...) la naturaleza de esos datos pertenece al núcleo esencial del derecho a la intimidad, entendido como aquella esfera o espacio de vida privada no susceptible de la interferencia arbitraria de las demás personas, que al ser considerado un elemento esencial del ser, se concreta en el derecho a poder actuar libremente en la mencionada esfera o núcleo, en ejercicio de la libertad personal y familiar, sin más limitaciones que los derechos de los demás y el ordenamiento jurídico”.

Por lo tanto, la definición de dato sensible no está solamente relacionada con la garantía propia del ejercicio del derecho de habeas data, sino que también va ligado al derecho fundamental a la intimidad, el cual, igualmente, es sujeto de protección constitucional.

Obrando en consecuencia con la importancia constitucional y legal atribuida al dato sensible, el legislador estatutario, en el artículo 6 de la Ley 1581 de 2012 prohibió1 (sic) por regla general, el Tratamiento de información sensible de los Titulares, de tal forma que sólo consagró unas excepciones taxativas a dicha exclusión, las cuales responden a La (sic) necesidad de garantizar otros derechos constitucionales tales como la vida, la educación y el derecho de asociación.

Teniendo presente tal situación, el legislador estatutario dispuso que, para que el responsable del Tratamiento pueda tratar datos sensibles debe realizarlo conforme a lo establecido en el artículo 6 de la Ley 1581 de 2012 y además requiere que se le comunique al Titular que los datos que está pretendiendo recoger son sensibles y que no está obligado a entregarlos. Condiciones relevantes que garantizarán que el Titular entregue o no su consentimiento de manera informada, circunstancia esencial para que proceda el Tratamiento de los datos sensibles por parte del responsable de acuerdo con la ley.

En el presente caso, se evidenció que

9 “Artículo 6° (sic). 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 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 pan 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.”

Al respecto, es necesario citar el artículo 2.2.2.25.2.3 del Decreto 1074 de 201510, el cual reza lo siguiente:

ARTICULO 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 de la Ley 1581 de 2012 está prohibido, a excepción de los casos expresamente señalados en el artículo 6 de la citada ley.

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

- 1. Informar al titular que por tratarse de datos sensibles no está ligado 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, los cuales, estos 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.

De otra parte, y teniendo en cuenta que en nuestra operación hemos dado cumplimiento a las normas en materia de protección de datos personales, pues las autorizaciones exigidas por la ley las tenemos publicadas en la página con sus políticas, autorizaciones y declaraciones de exoneración.

Así las cosas en el caso que nos ocupa, no puede deducirse o simplemente concluirse que los Titulares al ingresar a la página web, se encuentran plenamente informados y conocen cual es la finalidad del Tratamiento dado a sus datos. (destacamos)

Finalmente, manifestamos que se modificaron los avisos de privacidad de la siguiente manera:

Como se evidencia en la siguiente imagen traída de la página web de la entidad se hicieron los cambios pertinentes como son:

- La casilla de tratamiento de datos personales ya no viene marcada por defecto.
- Se habilitó para el conocimiento de las personas de forma inmediata la Política de Tratamiento de Datos personales de la entidad.
- Al mismo tiempo le damos a conocer a través de un mensaje que aparece cuando se ubica el cursor que debe aceptar la política de tratamiento ya que los datos depositados no son datos sensibles según lo estipulado por la Ley 1581 de 2012.

The image shows a registration form with the following elements:

- Tipo de Persona**: A dropdown menu with the placeholder text "Seleccione una opción".
- Nombre**: A text input field.
- Apellidos**: A text input field.
- Correo Electrónico**: A text input field.
- Contraseña**: A text input field.
- Repita la Contraseña**: A text input field.
- ☐ **Autorizo a la Cámara de Comercio de Córdoba** tratar mis datos personales para su gestión interna, conforme a su **Política de Protección de Datos Personales**. [Ver política de tratamiento de datos.](#)
- Registrarse**: A green button.
- A message box at the bottom: **Para registrarse necesitamos que acepte nuestra politica de tratamiento de datos**.

Otro de los cambios hechos fue el de formulario de Google como se evidencia en la siguiente imagen:

Los cambios pertinentes como son:

- Se agregó la casilla de tratamiento de datos personales y de igual forma ya no viene marcada por defecto.
- Se habilitó para el conocimiento de las personas de forma inmediata la Política de Tratamiento de Datos personales de la entidad.
- Al mismo tiempo le damos a conocer a través de un mensaje que aparece cuando se ubica el cursor que debe aceptar la política de tratamiento ya que los datos depositados no son datos sensibles según lo estipulado por la Ley 1581 de 2012.
- Se habilitó de forma inmediata la opción de supresión, reclamo o actualización de la información mediante el Formato de Reclamación de Datos Personales.

Para el formulario de PQRS de la página, se hizo un cambio en la navegación de la página el cual no lleva directamente al formulario de PQRS sino que lo lleva primero a que autorice el tratamiento de datos personales cumpliendo así con lo estipulado en la ley 1581 de 2012 como se evidencia en las siguientes imágenes:



Este enlace nos lleva a que la persona autorice el tratamiento de datos personales como se evidencia en la siguiente imagen:



En la imagen anterior se pueden observar cambios pertinentes como son:

- Se agregó la casilla de tratamiento de datos personales y de igual forma ya no viene marcada por defecto.
- Se habilitó para el conocimiento de las personas de forma inmediata la Política de Tratamiento de Datos personales de la entidad.

Así las cosas, y teniendo en cuenta que la entidad investigada ya procedió a ajustar el aviso de privacidad en la página web respecto de la recolección de datos personales, solicitamos desestimar los cargos imputados.

Respecto al deber de conservar la información bajo las condiciones de seguridad necesarias para evitar el uso y acceso de personas no autorizadas aun cuando, negar al Titular el acceso a las bases de datos donde reposa su información personal, implicaría en principio una violación a su derecho de habeas data, el artículo 15 de la Constitución Política debe interpretarse de manera armónica con los principios de circulación restringida y de seguridad. Así, se debe tener presente que los responsables del Tratamiento deben garantizar, entre otras cosas, que la información personal no sea publicada en internet, salvo que exista previamente una autorización por parte del Titular. Ahora bien, aun existiendo el consentimiento de éste, la divulgación, circulación y acceso de los datos tiene que estar controlado y restringido frente a terceros no autorizados, razón por la cual la ley ha impuesto a los responsables del Tratamiento una serie de deberes encaminados a dicho fin, como lo es el de “conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento”

Precisamente el artículo 4 de la Ley 1581 de 2012 establece los principios para el Tratamiento de los datos personales, entre los cuales se encuentran el principio de seguridad que señala lo siguiente:

g) PRINCIPIO DE SEGURIDAD: 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;

Como se advierte, el principio de seguridad debe ser cumplido por los responsables y Encargados del Tratamiento para garantizar el derecho de habeas data de los Titulares, pues de la adopción de medidas de conservación de la información y de los controles de seguridad implementados depende que se minimicen los riesgos de filtración de los datos personales.

Al respecto, esta entidad debe precisar, que la adopción de medidas necesarias para salvaguarda los datos personales de los Titulares, se debe observar teniendo en cuenta factores como el volumen de la información alojada en la base de datos a la que se le realiza el Tratamiento, como la naturaleza de los datos que trata, por lo cual dichos controles deberán ser directamente proporcionales al tipo de base de datos. De esta manera y teniendo una infraestructura tecnología controlada no se genera algún riesgo al que se expondrían las bases de datos y por ende la información personal en ellas contenida, al tener debidamente actualizados y ejecutados la protección de nuestro sistema.

Ahora bien, es de enfatizar que la Cámara de Comercio de Montería cuenta con unas Políticas, procedimientos y formatos de protección de datos personales que permiten evitar que se materializasen los posibles riesgos a que haya lugar, documentos que se pueden encontrar en nuestra página web en la sección de ley de transparencia.

Así las cosas, y de conformidad a las modificaciones realizadas por esta entidad investigada, solicitamos muy respetuosamente a esta Superintendencia que desestime el cargo imputado y archive la investigación administrativa de la referencia por todas las consideraciones expuestas.

SÉPTIMO: Que mediante Resolución 74979 del 24 de noviembre de 2020, esta Dirección incorporó las pruebas obrantes en la totalidad del expediente radicado bajo el número 20-221040, con el valor legal correspondiente, declarando agotada la etapa probatoria, corriendo traslado a la investigada para que presentara los alegatos de conclusión respectivos.

OCTAVO: Que la Resolución 74979 del 24 de noviembre de 2020 fue comunicada al Presidente Ejecutivo de la **CÁMARA DE COMERCIO** el 25 de noviembre de 2020, según consta en la certificación expedida el Coordinador del Grupo de Notificaciones y Certificaciones de esta Superintendencia, radicada bajo el número 20-221040-14, de fecha 14 de diciembre de 2020.

NOVENO: Que, dentro del término concedido para el efecto, el apoderado de la **CÁMARA DE COMERCIO** presentó alegatos de conclusión, bajo el radicado 20-221040-13 del 9 de diciembre de 2020, mediante los cuales reitera los argumentos presentados en el escrito de descargos.

DÉCIMO: Que de conformidad con lo expuesto en la presente actuación administrativa, y de conformidad con lo establecido en el artículo 19 de la Ley 1581 de 2012, se presentan las siguientes:

CONSIDERACIONES DE LA DIRECCIÓN DE INVESTIGACIÓN DE PROTECCIÓN DE DATOS PERSONALES

1. PRECISIONES PRELIMINARES.

El Presidente Ejecutivo de la **CÀMARA DE COMERCIO**, solicita en el escrito de descargos el archivo de la presente actuación, en la medida que los hallazgos descritos por el Despacho en el acto administrativo que formuló los cargos fueron debidamente subsanados, por lo que no existe fundamento alguno para la imposición de una sanción.

De conformidad con lo anteriormente indicado, este Despacho se pronunciará respecto de los deberes relacionados en los literales b) y c) del artículo 17 de la Ley 1581 de 2012, posteriormente se referirá respecto de la Responsabilidad Demostrada, para finalmente analizar si para el caso que nos ocupa, se impondrá una sanción de carácter pecuniaria.

2. DEL DEBER DE SOLICITAR Y CONSERVAR LA RESPECTIVA AUTORIZACIÓN OTORGADA POR EL TITULAR.

El artículo 15 de la Constitución Política, establece que “[t]odas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas”.

Dicha norma establece que las personas, en desarrollo de su derecho a la autodeterminación informática y al principio de libertad, son quienes de forma expresa deben autorizar que la información que sobre ellos sea recaudada pueda ser incluida en una base de datos.

En desarrollo de lo anterior, el literal b) del artículo 17 la Ley 1581 de 2012 le impone a los Responsables del Tratamiento de Datos Personales el deber de “[s]olicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular”;

Respecto de la autorización para el tratamiento de datos personales, el artículo 9 de la mencionada Ley, dispone:

ARTÍCULO 9o. AUTORIZACIÓN DEL TITULAR. Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.

El Decreto 1074 de 2015, a través de los artículos 2.2.2.25.2.4 y 2.2.2.25.2.5 en lo que tiene que ver con el modo de obtener la autorización y su prueba, dispone lo siguiente:

“Artículo 2.2.2.25.2.4. Modo de obtener la autorización. Para efectos de dar cumplimiento a lo dispuesto en el artículo 9 de la Ley 1581 de 2012, los Responsables del Tratamiento de datos personales establecerán mecanismos para obtener la autorización de los titulares o de quien se encuentre legitimado de conformidad con lo establecido en el artículo 2.2.2.25.2.1, del presente Decreto, que garanticen su consulta. Estos mecanismos podrán ser predeterminados a través de medios técnicos que faciliten al Titular su manifestación automatizada.

Se entenderá que la autorización cumple con estos requisitos cuando se manifieste (i) por escrito (ii) de forma oral o (iii) mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca.

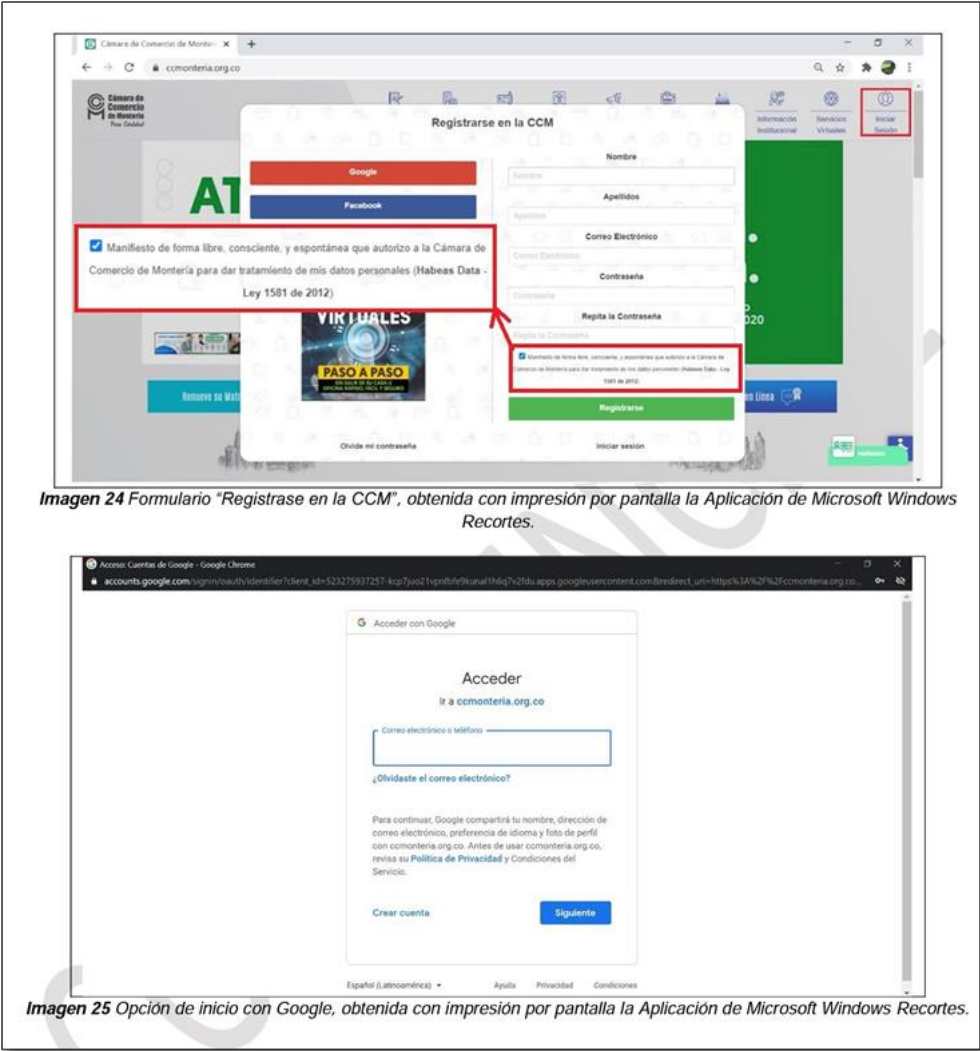
Artículo 2.2.2.25.2.1 Prueba de la autorización. Los Responsables deberán conservar prueba de la autorización otorgada por los titulares de datos personales para el Tratamiento de los mismos”.

De conformidad con las normas anteriormente citadas, el Responsable del tratamiento debe solicitar al titular de la información la respectiva autorización, que no es otra cosa, que poner en su conocimiento que sus datos personales serán tratados conforme a las normas legales; dicha autorización debe ser solicitada en todos los casos excepto aquellos que estén relacionados en el artículo 10 de la Ley 1581 de 2012.

Pues bien, este Despacho conforme a las conclusiones hechas en el Acta de Preservación de la página web de la **CÁMARA DE COMERCIO**, consideró que no obstante al navegar por el sitio www.ccomonteria.org se encuentran varios formatos de autorización para el tratamiento de datos personales, éstas no se encontraban disponibles al momento de la recolección directa de los Datos por medio de los formularios (i) Formulario “Registrarse en la CCM” y (ii) Formulario “Solicitud PQR’S”.

(i) Formulario “Registrarse en la CCM”

En lo que tiene que ver con el formulario “Registrarse en la CCM”, la autorización para el tratamiento de datos personales se encuentra en una “*caja de verificación la cual está marcada por defecto*”. Igualmente ofrece la posibilidad de iniciar el registro a través de una cuenta de Google o de Facebook, pero no se indica nada respecto de la autorización que debe dar el titular de la información.



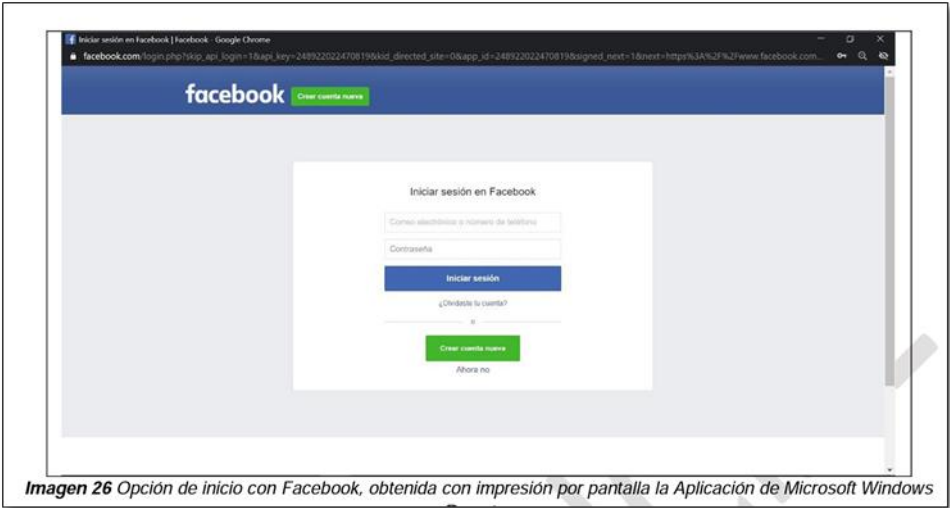


Imagen 26 Opción de inicio con Facebook, obtenida con impresión por pantalla la Aplicación de Microsoft Windows

Así las cosas, considera este Despacho que la **CÁMARA DE COMERCIO** respecto del formulario “Registrarse en la CCM”, no cumplió con el deber establecido en el literal b) del artículo 17 de la Ley 1581 de 2012.

(ii) Formulario “Solicitud PQR’S”

En la ya citada Acta de Preservación No. 068 del 17 de julio de 2020, se logra verificar que, respecto del formulario, “no contiene ningún tipo de aviso o aceptación para el tratamiento de datos personales”. Veamos:

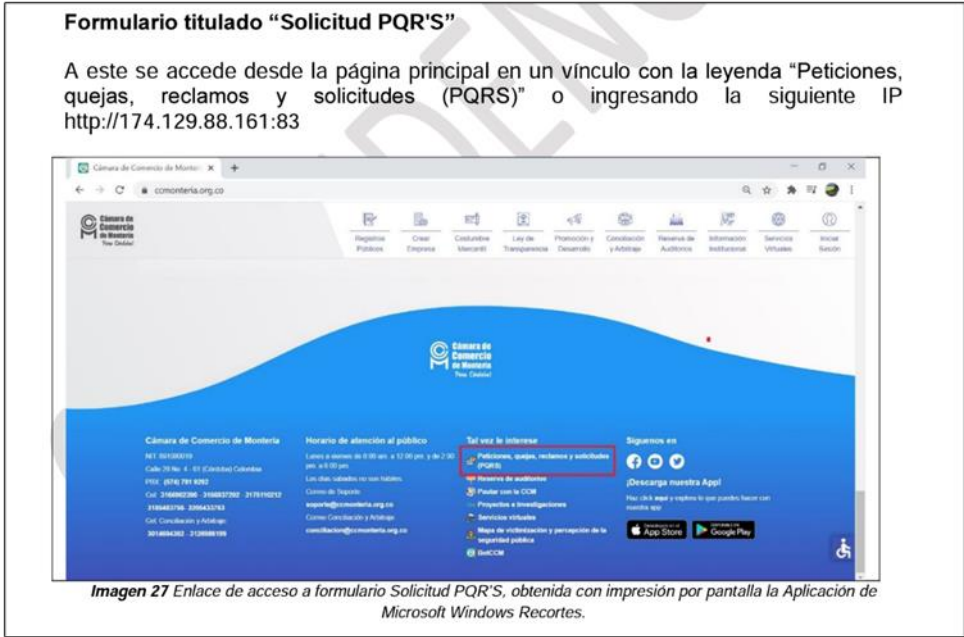


Imagen 27 Enlace de acceso a formulario Solicitud PQR'S, obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes.



Como pudo verificar el Despacho en el acto administrativo que formuló los cargos en el citado formulario de registro, no se solicita a los titulares que pretendan acceder al mismo la autorización para el tratamiento de sus datos personales. Por lo que la **CÁMARA DE COMERCIO** tampoco cumple con el deber de solicitar la autorización respecto del citado formulario.

En consecuencia, y en la medida que se logra determinar que hubo vulneración al Régimen de Protección de Datos Personales en relación con el deber establecido en el literal b) del artículo 17 de la Ley 1581 de 2012, por parte de la **CÁMARA DE COMERCIO**, se impondrá la sanción correspondiente.

3. DEL DEBER DE INFORMAR AL TITULAR SOBRE LA FINALIDAD DE LA RECOLECCIÓN Y LOS DERECHOS QUE LE ASISTEN POR VIRTUD DE LA AUTORIZACIÓN OTORGADA.

Establece el literal c) del artículo 17 de la Ley 1581 de 2012, 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:

c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada;

Así mismo, el artículo 12 de la misma norma, indica:

“ARTÍCULO 12. DEBER DE INFORMAR AL TITULAR. El Responsable del Tratamiento, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente:

a) **El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo;**

b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes;

c) Los derechos que le asisten como Titular;

d) La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.

PARÁGRAFO. El Responsable del Tratamiento deberá conservar prueba del cumplimiento de lo previsto en el presente artículo y, cuando el Titular lo solicite, entregarle copia de esta”.

A su vez, el artículo 2.2.2.25.2.1 del Decreto Único Reglamentario 1074 de 2015, establece:

“Artículo 2.2.22.25.2.1. Recolección de los datos Personales. En desarrollo de los principios de finalidad y libertad, la recolección de datos deberá limitarse a aquellos datos personales que son pertinentes y adecuados para la finalidad para la cual son recolectados o requeridos conforme a la normatividad vigente. Salvo en los casos expresamente previstos en la Ley, no se podrán recolectar datos personales sin autorización del Titular.

A solicitud de la Superintendencia de Industria y Comercio, los Responsables deberán proveer una descripción de los procedimientos usados para la recolección, almacenamiento, uso, circulación y supresión de información, como también la descripción de las finalidades para las cuales la información es recolectada y una explicación sobre la necesidad de recolectar los datos en cada caso.

No se podrán utilizar medios engañosos o fraudulentos para recolectar y realizar Tratamiento de datos personales”. (destacamos)

En relación el principio de finalidad, la Corte Constitucional mediante sentencia C- 748 de 2011, manifestó:

“Principio de finalidad: En virtud de tal principio, el tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley, la cual debe ser informada al titular.

La definición establecida por el legislador estatutario responde a uno de los criterios establecidos por la Corporación para el manejo de las bases de datos. Sin embargo, debe hacerse algunas precisiones.

Por una parte, los datos personales deben ser procesados con un propósito específico y explícito. En ese sentido, la finalidad **no sólo debe ser legítima** sino que la referida información se destinará a realizar los **fines exclusivos** para los cuales fue entregada por el titular. Por ello, se deberá informar al Titular del dato de manera clara, suficiente y previa acerca de la finalidad de la información suministrada y por tanto, no podrá recopilarse datos sin la clara especificación acerca de la finalidad de los mismos. Cualquier utilización diversa, **deberá ser autorizada en forma expresa por el Titular.**

Esta precisión es relevante en la medida que permite un control por parte del titular del dato, en tanto le es posible verificar si está siendo usado para la finalidad por él autorizada. Es una herramienta útil para evitar arbitrariedades en el manejo de la información por parte de quien trata el dato.

Así mismo, los datos personales deben ser procesados sólo en la forma que la persona afectada puede razonablemente prever. Si, con el tiempo, el uso de los datos personales cambia a formas que la persona razonablemente no espera, debe obtenerse el consentimiento previo del titular.

Por otro lado, de acuerdo la jurisprudencia constitucional y los estándares internacionales relacionados previamente, se observa que el principio de finalidad implica también: **(i) un ámbito temporal**, es decir que el periodo de conservación de los datos personales no exceda del necesario para alcanzar la necesidad con que se han registrado y **(ii) un ámbito material**, que exige que los datos recaudados sean los estrictamente necesarios para las finalidades perseguidas.

En razón de lo anterior, el literal b) debe ser entendido en dos aspectos.

Primero, bajo el principio de necesidad se entiende que los datos deberán ser conservados en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que fueron recogidos. Es decir, el periodo de conservación de los datos personales no debe exceder del necesario para alcanzar la necesidad con que se han registrado.

En la Sentencia **C-1011 de 2008**^{[228]1}, la Corporación reiteró la importancia de la existencia de unos criterios razonables sobre la permanencia de datos personales en fuentes de información. Además, sostuvo que este periodo se encuentra en una estrecha relación con la finalidad que pretende cumplir. Así, a partir del estudio de la jurisprudencia, construyó una doctrina constitucional comprehensiva sobre la caducidad del dato negativo en materia financiera y concluyó que dentro de las prerrogativas mismas del derecho al habeas data, se encuentra esta garantía, como una consecuencia del derecho al olvido. Sobre el particular observó la providencia:

“De acuerdo con lo señalado en el artículo 15 Superior, la Corte identifica como facultades que conforman el contenido del derecho al hábeas data, las de (i) conocer la información personal contenida en las bases de datos, (ii) solicitar la actualización de dicha información a través de la inclusión de nuevos datos y (iii) requerir la rectificación de la información no ajustada a la realidad. Junto con las prerrogativas expuestas, la Corte, habida cuenta los precedentes jurisprudenciales anteriores que señalaban la necesidad de establecer un límite al reporte financiero negativo, estableció un nuevo componente del derecho al hábeas data, la de la caducidad del dato negativo.”

(...)

La Corte reitera que los procesos de administración de datos personales de contenido crediticio cumplen un propósito específico: ofrecer a las entidades que ejercen actividades de intermediación

¹[228] M.P. Jaime Córdoba Triviño

financiera y, en general, a los sujetos que concurren al mercado, información relacionada con el grado de cumplimiento de las obligaciones suscritas por el sujeto concernido, en tanto herramienta importante para adoptar decisiones sobre la suscripción de contratos comerciales y de crédito con clientes potenciales. Esta actividad es compatible con los postulados superiores, pues cumple con propósitos legítimos desde la perspectiva constitucional, como son la estabilidad financiera, la confianza en el sistema de crédito y la protección del ahorro público administrado por los establecimientos bancarios y de crédito.

Es precisamente la comprobación acerca de la finalidad específica que tienen los operadores de información financiera y crediticia la que, a su vez, permite determinar los límites al ejercicio de las actividades de acopio, tratamiento y divulgación de datos.”
(Resaltado fuera del texto)

Segundo, los datos personales registrados deben ser los estrictamente necesarios para el cumplimiento de las finalidades perseguidas con la base de datos de que se trate, de tal forma que se encuentra prohibido el registro y divulgación de datos que no guarden estrecha relación con el objetivo de la base de datos. En consecuencia, debe hacerse todo lo razonablemente posible para limitar el procesamiento de datos personales al mínimo necesario. Es decir, los datos deberán ser: **(i)** adecuados, **(ii)** pertinentes y **(iii)** acordes con las finalidades para las cuales fueron previstos”.

Conforme a lo anteriormente indicado, sólo podrá ser recolectada aquella información que sea **imprescindible** para cumplir con la **finalidad del tratamiento**. Finalidad que, deberá ser informada de manera clara y expresa al titular de la información al momento en que es otorgada la autorización.

Así, los deberes de solicitar la autorización previa al tratamiento de los datos y el de informar la finalidad para la cual son recolectados, se encuentran estrechamente relacionados, en la medida que el titular **autoriza** el tratamiento de su información **de acuerdo con la finalidad que se le vaya a dar la misma**. Al mismo tiempo deberá informársele al titular respecto de los derechos que le asisten.

Este Despacho al verificar nuevamente las conclusiones relacionadas en el Acta de Preservación de la Página web de la **CÁMARA DE COMERCIO**, encontró que en lo que tiene que ver con los formularios estudiados no informa a los titulares la finalidad por la cual es recolectada la información solicitada.

8. Al momento de solicitar autorización para el Tratamiento de datos personales en cada uno de los formularios identificados en la página o aplicación inspeccionada, ¿se informan las finalidades del Tratamiento o se re-direcciona al documento en el que se encuentran plasmadas?

Formulario “Registrarse en la CCM”: contiene un aviso de información el cual no está enlazado con la Política de protección de datos personales o con el Formato de privacidad y autorización expresa para el tratamiento de datos personales.

Formulario “Solicitud PQR’S” Este no contiene ningún enlace a la Política de protección de datos personales o al Formato de privacidad y autorización expresa para el tratamiento de datos personales.

Así las cosas, y en lo que tiene que ver con lo establecido en el literal c) del artículo 17 de la Ley 1581 de 2012, se impondrá la sanción correspondiente, en la medida que la **CÁMARA DE COMERCIO**, incumplió con el citado deber, respecto de los formularios **(i)** Formulario “Registrarse en la CCM” y **(ii)** Formulario “Solicitud PQR’S”.

4. CARGO FORMULADO EN EL ARTÍCULO SEGUNDO DE LA RESOLUCIÓN 51634 DEL 28 DE AGOSTO DE 2020.

Dispuso el Despacho en la Resolución 51634 del 28 de agosto de 2020, lo siguiente:

ARTÍCULO SEGUNDO. FORMULAR PLIEGO DE CARGOS contra la Cámara de Comercio de Montería identificada con el Nit. 891080019 por el presunto incumplimiento del deber de informar al Titular al momento de solicitar la Autorización lo establecido en los literales a); b); c); y d) del artículo 12 de la Ley 1581 de 2012, en concordancia con los literales b); c) y e) del artículo 8 de la misma norma.

Pues bien, en la medida que, cuando se analizó el incumplimiento de las normas relacionadas en el Cargo formulado en el **ARTÍCULO TERCERO** del citado acto administrativo, se concluyó que respecto de los formularios **(i)** Formulario “Registrarse en la CCM” y **(ii)** Formulario “Solicitud PQR’S”, la **CÁMARA DE COMERCIO** no informó a través de los canales correspondientes la

finalidad con la cual son recolectados los datos personales de sus usuarios, este Despacho procederá al Archivo del Cargo relacionado en el **ARTÍCULO SEGUNDO**.

5. POTESTAD SANCIONATORIA DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. PROPORCIONALIDAD DE LA SANCIÓN

- **Aplicación del artículo 49 de la Ley 1955 de 2019.**

El artículo 49 de la Ley 1955 de 2019, mediante la cual se expide el Plan Nacional de Desarrollo 2018-2022, establece lo siguiente:

ART. 49. —Cálculo de valores en UVT. A partir del 1º de enero de 2020, todos los cobros, sanciones, multas, tasas, tarifas y estampillas, actualmente denominados y establecidos con base en el salario mínimo mensual legal vigente, SMMLV, deberán ser calculados con base en su equivalencia en términos de la unidad de valor tributario, UVT. En adelante, las actualizaciones de estos valores también se harán con base en el valor de la UVT vigente.

PAR. —Los cobros, sanciones, multas, tasas, tarifas y estampillas, que se encuentren ejecutoriados con anterioridad al 1º de enero de 2020 se mantendrán determinados en SMMLV.

De esta manera y de conformidad con la norma antes señalada, si el valor de los cobros, sanciones o multas se encuentran establecidos en salarios mínimos, estos deberán ser calculados con base en su equivalencia en términos de la unidad de valor tributario UVT. Por lo cual, las multas de carácter personal e institucional dispuestas en la Ley 1581 de 2012, serán determinadas de la siguiente manera:

$$\frac{\text{SMLV}}{\text{UVT vigente 2021}} = \text{Multa en UVT}$$

La Corte Constitucional a través de sentencia C-557 de 2000, señaló que la ley aprobatoria del Plan Nacional de Desarrollo tiene la siguiente naturaleza:

Partiendo de la concepción que entiende la planeación como el instrumento fundamental para el manejo económico del Estado, y con base en lo dispuesto por el inciso tercero del artículo 341 de la Constitución Política según el cual “(e)l Plan Nacional de Inversiones se expedirá mediante una ley que tendrá prelación sobre las demás leyes”, y que “sus mandatos constituirán mecanismos idóneos para su ejecución y suplirán los existentes sin necesidad de la expedición de leyes posteriores”, la jurisprudencia ha destacado que la Ley del Plan de Desarrollo, que debe expedirse en cada período presidencial, determina el contenido de las leyes anuales de presupuesto, de otras leyes que tocan el tema económico, social o ambiental (...)”

El Plan Nacional de Desarrollo por ser una ley de iniciativa gubernamental y de un amplio consenso - tanto en la elaboración del proyecto de Ley como en su trámite legislativo- su cumplimiento debe hacerse de manera inmediata por parte de todas las entidades de orden nacional². Su cumplimiento se mide en la ejecución que se haga del Plan Nacional de Desarrollo dentro las competencias que le sean propias a cada una de las entidades del orden nacional observando los criterios de concurrencia, complementariedad y subsidiariedad.

En consecuencia, cualquier norma que se incluya dentro del Plan Nacional de Desarrollo debe ser de obligatorio cumplimiento por las entidades que conforman la rama ejecutiva del nivel nacional a través del respectivo plan de acción institucional como lo establece el inciso 1 del artículo 26 de la ley 152 de 1994.

- **Potestad Sancionadora de esta Superintendencia.**

Frente al procedimiento para imponer las sanciones, el artículo 22 de la Ley 1581 de 2012 señaló:

“ARTÍCULO 22. TRÁMITE. La Superintendencia de Industria y Comercio, una vez establecido el incumplimiento de las disposiciones de la presente ley por parte del Responsable del Tratamiento o el Encargado del Tratamiento, adoptará las medidas o impondrá las sanciones correspondientes”.

Respecto de la “Potestad sancionatoria” que ejerce la administración, la Corte Constitucional ha señalado:

“El poder sancionador estatal ha sido definido como “un instrumento de autoprotección, en cuanto contribuye a preservar el orden jurídico institucional mediante la asignación de competencias a la administración que la

² Las entidades territoriales tienen sus propios Planes de Desarrollo, artículos 31 y ss., de la Ley 152 de 1994. Sin perjuicio, a la participación que éstas tienen en la elaboración del PND.

habilitan para imponer a sus propios funcionarios y a los particulares el acatamiento, inclusive por medio punitivos, de una disciplina cuya observancia contribuye a la realización de sus cometidos.

Esa potestad es una manifestación del *jus punendi*, razón por la que está sometida a los siguientes principios: (i) el principio de legalidad, que se traduce en la existencia de una ley que la regule; es decir, que corresponde sólo al legislador ordinario o extraordinario su definición. (ii) El principio de tipicidad que, si bien no es igual de riguroso al penal, sí obliga al legislador a hacer una descripción de la conducta o del comportamiento que da lugar a la aplicación de la sanción y a determinar expresamente la sanción. (iii) El debido proceso que exige entre otros, la definición de un procedimiento, así sea sumario, que garantice el debido proceso y, en especial, el derecho de defensa, lo que incluye la designación expresa de la autoridad competente para imponer la sanción. (iv) El principio de proporcionalidad que se traduce en que la sanción debe ser proporcionalidad a la falta o infracción administrativa que se busca sancionar. (v) La independencia de la sanción penal; esto significa que la sanción se puede imponer independientemente de si el hecho que da lugar a ella también puede constituir infracción al régimen penal.³

En el mismo sentido, y en relación con los principios⁴ señalados, dicha corporación por medio de la sentencia C-948 de 2002 manifestó:

“En la doctrina^[36]⁵ se postula, así mismo, sin discusión que la administración o las autoridades titulares de funciones administrativas lo sean de potestad sancionadora y que ésta en cuanto manifestación del *ius puniendi* del Estado está sometida a claros principios generalmente aceptados, y en la mayoría de los casos proclamados de manera explícita en los textos constitucionales. Así, a los principios de configuración del sistema sancionador como los de legalidad (toda sanción debe tener fundamento en la ley), tipicidad (exigencia de descripción específica y precisa por la norma creadora de las infracciones y de las sanciones, de las conductas que pueden ser sancionadas y del contenido material de las sanciones que puede imponerse por la comisión de cada conducta, así como la correlación entre unas y otras) y de prescripción (los particulares no pueden quedar sujetos de manera indefinida a la puesta en marcha de los instrumentos sancionatorios), se suman los propios de aplicación del sistema sancionador, como los de culpabilidad o responsabilidad según el caso – régimen disciplinario o régimen de sanciones administrativas no disciplinarias- (juicio personal de reprochabilidad dirigido al autor de un delito o falta^[37]⁶), de proporcionalidad o el denominado *non bis in idem*”.

Ahora, al hacer referencia al principio de legalidad en materia de protección del derecho de habeas data, la Corte Constitucional mediante Sentencia C-1011 de 2008, manifestó:

“Para la Corte, en consecuencia, la flexibilidad que puede establecer el legislador en materia de derecho administrativo sancionador es compatible con la Constitución, siempre que esta característica no sea tan amplia que permita la arbitrariedad de la administración. Un cierto grado de movilidad a la administración para aplicar las hipótesis fácticas establecidas en la ley guarda coherencia con los fines constitucionales de esta actividad sancionatoria administrativa, en la medida que le permite cumplir eficaz y eficientemente con las obligaciones impuestas por la Carta. Sin embargo, ha advertido que la flexibilidad del principio de legalidad no puede tener un carácter extremo, al punto que se permita la arbitrariedad de la administración en la imposición de las sanciones o las penas^[203]⁷”.

De esta manera, no puede la administración sobrepasar los límites que le impone el legislador al momento de aplicar una sanción, es decir, que la conducta que está siendo investigada debe tener una connotación sancionable por mandato legal. En este punto es relevante el **principio de tipicidad**, el cual no es otra cosa que “la exigencia de una descripción específica y precisa por la norma creadora de las infracciones y de las sanciones, de las conductas que pueden ser sancionadas y del contenido material de las sanciones que puede imponerse por la comisión de cada conducta, así como la correlación entre unas y otras”⁸.

Sobre el citado principio de tipicidad, la Corte Constitucional mediante Sentencia C-748 de 2011 sostuvo:

“En relación con el principio de tipicidad, encuentra la Sala que pese a la generalidad de la ley, es determinable la infracción administrativa en la medida en que se señala que la constituye el **incumplimiento de las disposiciones de la ley**, esto es, en términos específicos, la regulación que hacen los artículos 17 y 18 del proyecto de ley, en los que se señalan los deberes de los responsables y encargados del tratamiento del dato”.

Entonces, es suficiente desconocer cualquiera de las disposiciones contempladas en la Ley 1581 de 2012, para que se pueda ejercer su potestad sancionatoria, eso sí, en los casos en los que así lo

³ Corte Constitucional. Sentencia C-748 de 2011
⁴ “Los principios señalados en el CPACA tienen un carácter normativo y vinculante, a diferencia de la naturaleza orientadora que se predicaba en el CCA. La aplicabilidad general de los principios previstos en el artículo 3° del CPACA, como desarrollo directo de la Constitución Política, conlleva a que dichos principios deban observarse para cualquier actuación administrativa, incluidas las reguladas en leyes especiales. Así las cosas, el intérprete deberá utilizarlos directamente o hacer un ejercicio de integración normativa, entre los principios de la actuación administrativa previstos en la ley especial y los señalados en el CPACA”. Laverde A. JUAN MANUEL. Manual de Procedimiento Administrativo Sancionatorio. Ed. Legis S.A. Bogotá Colombia Segunda Edición 2018.p. 51
⁵ [36] Juan Alfonso Santamaría Pastor. Principios de Derecho Administrativo. Volumen II. Ed. Centro de Estudios Ramón Areces. Madrid. Tomo II. Segunda Edición. 2000.
⁶ [37] Ver Ramón Parada Vásquez. Derecho Administrativo. Tomo I Marcial Pons. Madrid 1996. Luis Morell Ocaña. Curso de Derecho Administrativo. Tomo II “La actividad de las administraciones públicas. Su control administrativo y jurisdiccional”. Arandazi. Madrid. 1996.
⁷ [203] Sentencia C-406 de 2004.
⁸ Sentencias C-827 de 2001 y C-343 de 2006.

determine la actuación administrativa correspondiente, como consecuencia directa de la trasgresión de las normas que amparan el derecho fundamental de habeas data. Principalmente, cuando se trata de las disposiciones que se refieren a los deberes a los que están sujetos los Responsables o Encargados del tratamiento de la información.

Debe este Despacho precisar que las sanciones que se imponen dentro de procesos administrativos sancionatorios no constituyen una cuantificación de perjuicios materiales o morales, es decir no se trata de la cuantificación de un daño subjetivo, como sucede en el régimen civil de responsabilidad. Por el contrario, las sanciones que impone esta Superintendencia, en virtud del artículo 22 y siguientes de la Ley 1581 de 2012, son una consecuencia negativa impuesta en contra de la persona natural o jurídica que viole las disposiciones de la Ley; tienen como fin central proteger y promover el respeto del derecho fundamental a la protección de datos personales, derecho humano (universal, inalienable, indivisible, irrenunciable e imprescriptible) que fue positivizado por el Constituyente Primario en el artículo 15 de la Constitución de 1991, y que en muchas ocasiones es conexo a otros derechos fundamentales de gran relevancia constitucional como la dignidad humana, el buen nombre, la intimidad, etc.

La vulneración del derecho fundamental a la protección de datos personales no solo afecta los derechos de una persona en particular, sino que pone en riesgo los derechos fundamentales de toda la sociedad. Por eso, las sanciones de dichas conductas no pueden, ni deben tratarse, como una cuestión insignificante o de poca monta. La transgresión flagrante a los derechos humanos de un ciudadano es, por sí sólo, un hecho muy grave que no necesita de forzosos razonamientos para evitar un desentendimiento de la importancia de lo sucedido.

Recuérdese que, según la Declaración Universal de los Derechos Humanos, “el desconocimiento y el menosprecio de los derechos humanos han originado actos de barbarie ultrajantes para la conciencia de la humanidad”⁹. Por eso, según dicho documento, se considera “esencial que los derechos humanos sean protegidos por un régimen de Derecho”. No debe olvidarse que el respeto de los derechos humanos es un elemento esencial de la democracia¹⁰.

De conformidad con lo anteriormente indicado, este Despacho procederá a determinar la sanción a imponer y la graduación de la misma.

• **Imposición de la Sanción al caso concreto.**

Los artículos 23 y 24 de la Ley 1581 de 2012, establecen las sanciones que podrá imponer esta entidad, así como los criterios en que éstas deberán ser graduadas, veamos:

ARTÍCULO 23. SANCIONES. La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:

- a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;
- b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;
- c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;
- d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles;

PARÁGRAFO. Las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva.

ARTÍCULO 24. CRITERIOS PARA GRADUAR LAS SANCIONES. Las sanciones por infracciones a las que se refieren el artículo anterior, se graduarán atendiendo los siguientes criterios, en cuanto resulten aplicables:

- a) La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley;
- b) El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción;
- c) La reincidencia en la comisión de la infracción;
- d) La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio;
- e) La renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio;
- f) El reconocimiento o aceptación expresas que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.

⁹ Organización de las Naciones Unidas (1948). Declaración Universal de los Derechos Humanos

¹⁰ Artículo 3 de la Carta Democrática Interamericana la cual se puede consultar en: http://www.oas.org/OASpage/esp/Documentos/Carta_Democratica.htm

De acuerdo con las consideraciones anteriormente hechas y de lo establecido en el literal a) del citado artículo 24, basta que la conducta desplegada por la investigada haya puesto en peligro los intereses jurídicos tutelados por la Ley 1581 de 2012, para la imposición de una sanción.

Para el caso que nos ocupa, quedó demostrado que la **CÁMARA DE COMERCIO**, vulneró los deberes contemplados en la Ley 1581 de 2012 razón por la que considera el Despacho procedente imponer una sanción de carácter pecuniario, como se indica a continuación:

i) El literal b) del artículo 17, en concordancia con el literal c) del artículo 4º y artículo 9º de la Ley 1581 de 2012 y el inciso primero del artículo 2.2.2.25.2.2 del Decreto Único Reglamentario 1074 de 2015; en la medida que respecto de los formularios **(i)** Registrarse en la CCM y **(ii)** Solicitud de PQR’S, la **CÁMARA DE COMERCIO** no solicitó la autorización de los titulares para el tratamiento de los datos personales recolectados.

Como consecuencia se impondrá la sanción pecuniaria de VEINTICINCO MILLONES CUATROCIENTOS QUINCE MIL SEISCIENTOS PESOS M/CTE (\$25.415.600), equivalente a 700 Unidades de Valor Tributario (UVT)

ii) El literal c) del artículo 17, en concordancia con el literal b) del artículo 4º, artículo 8º y artículo 12 de la Ley 1581 de 2012 y, el inciso primero del artículo 2.2.2.25.2.2. y artículo 2.2.2.25.2.3. del Decreto Único Reglamentario 1074 de 2015; en la medida que respecto de los **(i)** Registrarse en la CCM y **(ii)** Solicitud de PQR’S la **CÁMARA DE COMERCIO** no informa al Titular de manera clara y expresa la finalidad de la recolección de los datos personales, como tampoco los derechos que le asiste.

Como consecuencia se impondrá la sanción pecuniaria de VEINTICINCO MILLONES CUATROCIENTOS QUINCE MIL SEISCIENTOS PESOS M/CTE (\$25.415.600), equivalente a 700 Unidades de Valor Tributario (UVT)

• **Graduación de la Sanción Impuesta.**

El ya citado artículo 24 de la Ley 1581 de 2012, enumera los criterios que debe tener en cuenta la administración para la imposición de una sanción de carácter pecuniario. Al respecto, la Corte Constitucional en sentencia C – 748 de 2011, manifestó que, de dichos criterios, los relacionados en los literales a), b), c), d) y e) corresponden a los de agravación, determinando que únicamente el criterio relacionado en el literal f) será el de atenuación.

Pues bien, este Despacho para la imposición de la sanción tuvo en cuenta lo establecido en el literal a) del artículo 24 de la Ley 1581 de 2012, en la medida que, como se dijo, basta que la conducta o conductas investigadas hayan puesto en peligro los intereses jurídicos protegidos por la Ley. Cuando el Responsable del tratamiento no cumple con los deberes que le impone la Ley, vulnera el derecho de habeas data protegido por la Ley 1581 de 2012.

En lo que tiene que ver con los criterios señalados en los literales b), c) d) y e) del artículo 24 de la Ley 1581 de 2012 no fueron tenidos en cuenta debido a que dentro de la investigación realizada **(i)** no se encontró que la investigada hubiera obtenido beneficio económico alguno por la comisión de la infracción, **(ii)** no hubo reincidencia en la comisión de la infracción, **(iii)** no hubo resistencia u obstrucción a la acción Investigativa de la Superintendencia y, **(iv)** no hubo renuencia o desacato a cumplir las órdenes e instrucciones del Despacho.

El criterio de atenuación señalado en el literal f) del artículo 24 de la Ley 1581 de 2012 **no se aplicará** en la presente actuación administrativa, toda vez que la **CÁMARA DE COMERCIO**. en calidad de Responsable, en ninguna de las etapas de la presente actuación administrativa reconoce expresamente que respecto de los formularios relacionados anteriormente, **(i) no solicitó autorización del titular para el tratamiento de los datos personales (ii) no informó la finalidad de la recolección y los derechos que le asisten al titular por virtud de la autorización otorgada.**

6. RESPONSABILIDAD DEMOSTRADA (ACCOUNTABILITY) EN EL TRATAMIENTO DE DATOS PERSONALES.

La regulación colombiana le impone al Responsable o al Encargado del Tratamiento, la responsabilidad de garantizar la eficacia de los derechos del titular del dato, la cual no puede ser simbólica, ni limitarse únicamente a la formalidad. Por el contrario, debe ser real y demostrable. Al respecto, nuestra jurisprudencia ha determinado que “existe un deber constitucional de administrar

correctamente y de proteger los archivos y bases de datos que contengan información personal o socialmente relevante¹¹.

Adicionalmente, es importante resaltar que los responsables o encargados 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 Decreto 1074 de 2015, reglamenta algunos aspectos relacionados con el principio de responsabilidad demostrada.

El artículo 2.2.2.25.6.1¹² del citado Decreto, establece que *“los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012”*. Así, resulta imposible ignorar la forma en que el Responsable o Encargado del Tratamiento debe probar poner en funcionamiento medidas adecuadas, útiles y eficaces para cumplir la regulación. Es decir, se reivindica que un administrador 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.

A su vez, el artículo 2.2.2.25.6.2 del Decreto 1074 de 2015, exige que los responsables del tratamiento de datos implementen medidas efectivas y apropiadas que garanticen, entre otras: “(...) 2. La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación.”¹³

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 demostrada¹⁴(accountability)¹⁵”.

El término “accountability”¹⁶, 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:

¹¹ Cfr. Corte Constitucional, sentencia T-227 de 2003.

¹² El texto completo del artículo 2.2.2.25.6.1 del Decreto 1074 de 2015 establece: *“Demostración. Los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este decreto, en una manera que sea proporcional a lo siguiente:*

1. La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.
2. La naturaleza de los datos personales objeto del tratamiento.
3. El tipo de Tratamiento.
4. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares. En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, los Responsables deberán suministrar a esta una descripción de los procedimientos usados para la recolección de los datos personales, como también la descripción de las finalidades para las cuales esta información es recolectada y una explicación sobre la relevancia de los datos personales en cada caso.

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

¹³ El texto completo del artículo 2.2.2.25.6.2. del Decreto 1074 de 2015 señala: *“Políticas internas efectivas. En cada caso, de acuerdo con las circunstancias mencionadas en los numerales 1, 2, 3 y 4 del artículo 26 anterior, las medidas efectivas y apropiadas implementadas por el Responsable deben ser consistentes con las instrucciones impartidas por la Superintendencia de Industria y Comercio. Dichas políticas deberán garantizar:*

1. La existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable para la adopción e implementación de políticas consistentes con la Ley 1581 de 2012 y este decreto.
2. La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación.
3. La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del tratamiento. La verificación por parte de la Superintendencia de Industria y Comercio de la existencia de medidas y políticas específicas para el manejo adecuado de los datos personales que administra un Responsable será tenida en cuenta al momento de evaluar la imposición de sanciones por violación a los deberes y obligaciones establecidos en la ley y en el presente decreto”.

¹⁴ El texto de la guía puede consultarse en: <http://www.sic.gov.co/sites/default/files/files/Publicaciones/GuiaAccountability.pdf>

¹⁵ “El término “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.

¹⁶ Cfr. Grupo de trabajo de protección de datos del artículo 29. Dictamen 3/2010 sobre el principio de responsabilidad, pág. 8.

1. Diseñar y activar un programa integral de gestión de datos (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 naturaleza¹⁷ para garantizar el correcto cumplimiento de los deberes que imponen las regulaciones sobre tratamiento de datos personales. El mismo, exige que los responsables y encargados 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 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 indebido de sus datos personales**”¹⁸. (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.

Manifiesta el Presidente Ejecutivo de la **CÁMARA DE COMERCIO**, en el escrito de descargos, que, respecto de los hallazgos encontrados por parte de esta Superintendencia relacionados con la protección de datos personales se realizaron las modificaciones correspondientes, por lo que solicita sean desestimados los cargos formulados en la Resolución 51634 del 28 de agosto de 2020.

Pues bien, el ya citado artículo 2.2.2.25.6.2 del Decreto 1074 de 2015, establece: “*la verificación de la existencia de medidas y políticas específicas para el manejo adecuado de los datos personales que administra un responsable será tomada en cuenta al momento de evaluar la imposición de sanciones por violación a los deberes y obligaciones establecidos en la ley (...)*”.

A lo largo de la presente actuación administrativa, ha indicado el Despacho que la **CÁMARA DE COMERCIO** vulneró los deberes que como Responsables en el tratamiento de datos personales está llamada a cumplir. Los formularios **(i)** Registrarse en la CCM y **(ii)** Solicitud de PQR’S, corresponden a actividades propias de la entidad, por lo que, estaba en la obligación de solicitar de los titulares de

¹⁷ 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.
¹⁸ 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 información la autorización para el tratamiento, así como informar respecto de la finalidad de dicho tratamiento.

De acuerdo con lo informado en el escrito de Descargos, la implementación de medidas efectivas para la protección de los datos personales **sólo tuvo ocurrencia cuando la presente actuación administrativa ya había iniciado**, situación que no la exonera del cumplimiento de los deberes establecidos en la Ley 1581 de 2012, en su calidad de Responsable del tratamiento. La multiplicidad de mecanismos implementados debe servir para que todos los aspectos previstos en la norma como una obligación, se cumplan de manera eficiente y eficaz, lo cual no fue lo que resultó demostrado en el presente caso.

De conformidad con lo anteriormente indicado, este Despacho no tendrá en cuenta lo dispuesto en el parágrafo del artículo 2.2.2.25.6.2 del Decreto 1074 de 2015.

7. CONCLUSIONES.

Conforme a las consideraciones realizadas por el Despacho y de acuerdo con la valoración a las pruebas allegadas a la presente actuación, se archivará la presente actuación, teniendo en cuenta:

- a) La **CÁMARA DE COMERCIO**, no solicitó la autorización previa de que trata el artículo 9 de la Ley 1581 de 2012, respecto de los formularios evaluados (i) Registrarse en la CCM y (ii) Solicitud de PQR'S, vulnerando de esta manera el deber que como Responsable está obligado a cumplir relacionado en el literal b) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal c) del artículo 4 y el artículo 9 de la misma ley.
- b) La **CÁMARA DE COMERCIO**, tampoco informó a los titulares la finalidad con la cual es recolectada la información en los formularios evaluados (i) Registrarse en la CCM y (ii) Solicitud de PQR'S, vulnerando de esta manera el deber establecido en el literal c) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal b) del artículo 4, y el artículo 12 de la misma Ley.
- c) En lo que tiene que ver con el cargo formulado en el **ARTÍCULO SEGUNDO** de la Resolución 51634 del 28 de agosto de 2020, será archivado, en la medida que sobre la vulneración de las normas allí descritas se encuentran igualmente relacionadas en el **ARTÍCULO TERCERO** del citado acto administrativo, y sobre el cual se impuso la sanción correspondiente.
- d) La implementación de medidas en materia de protección de datos personales por parte de la **CÁMARA DE COMERCIO**, posterior al incumplimiento de los deberes que dio origen a la presente actuación administrativa, no la exonera de responsabilidad, por lo que no se tuvo en cuenta lo dispuesto en el parágrafo del artículo 2.2.2.25.6.2 del Decreto 1074 de 2015.

DÉCIMOPRIMERO: Que, en virtud de la situación actual, teniendo en cuenta el Estado de Emergencia Económica, Social y Ecológica decretado por el Gobierno Nacional, se ha restringido el ingreso a las instalaciones de la Superintendencia, en consecuencia, se establecieron las medidas pertinentes para permitir el acceso completo a los expedientes, por lo que la **CÁMARA DE COMERCIO**, deberá:

- (i) Enviar un correo electrónico a contactenos@sic.gov.co o habeasdata@sic.gov.co, solicitando el acceso al expediente a través de la plataforma servicios en línea, indicando: número de radicado, nombre completo de la persona que va a consultar el expediente, número de identificación y correo electrónico autorizado;
- (ii) Una vez reciba respuesta positiva respecto de la solicitud de acceso, la entidad debe registrarse en servicios en línea link <https://servicioslinea.sic.gov.co/servilinea/ServiLinea/Portada.php> y a través del mismo link posteriormente al registro puede consultar el expediente de manera digital.

No obstante, en aras de garantizar los derechos de defensa y contradicción de la investigada, en el caso en que la misma considere necesario el acceso del expediente en físico, deberá enviar un correo electrónico a la dirección de correo habeasdata@sic.gov.co, solicitando que le asignen una cita para que pueda examinar el expediente, con el número de la referencia, en las instalaciones de la Superintendencia de Industria y Comercio en la ciudad de Bogotá. Lo anterior por cuanto se deben garantizar el ingreso a las instalaciones con las adecuadas medidas de bioseguridad.

En mérito de lo expuesto, este Despacho.

RESUELVE

ARTÍCULO PRIMERO: IMPONER una sanción pecuniaria a la **CÁMARA DE COMERCIO DE MONTERIA**, identificada con el Nit.891.080.019-4 de **CINCUENTA MILLONES OCHOCIENTOS TREINTA Y UN MIL DOSCIENTOS PESOS MCTE** (\$50.831.200) equivalentes a **1400 UVT Unidad de Valor Tributario**, por la vulneración de lo dispuesto en las normas que se relacionan a continuación, respecto de los formularios **(i)** Registrarse en la CCM y **(ii)** Solicitud de PQR'S, así:

- i. El literal b) del artículo 17, en concordancia con el literal c) del artículo 4º y artículo 9º de la Ley 1581 de 2012 y el inciso primero del artículo 2.2.2.25.2.2 del Decreto Único Reglamentario 1074 de 2015.
- ii. El literal c) del artículo 17, en concordancia con el literal b) del artículo 4º, artículo 8º y artículo 12 de la Ley 1581 de 2012 y, el inciso primero del artículo 2.2.2.25.2.2. y artículo 2.2.2.25.2.3. del Decreto Único Reglamentario 1074 de 2015.

PARÁGRAFO: El valor de la sanción pecuniaria que por esta resolución se impone, deberá consignarse en efectivo o cheque de gerencia en el Banco Popular, Cuenta No. 050000249, a nombre de Dirección del Tesoro Nacional – Fondos Comunes, Código Rentístico No. 350300, Nit. 899999090-2. El pago deberá efectuarse dentro de los cinco (5) días hábiles siguientes a la ejecutoria de esta resolución y acreditarse en la ventanilla de Tesorería de esta Superintendencia con el original de la consignación, donde le expedirán el recibo de caja aplicado a la resolución sancionatoria. Vencido este plazo se cobrarán intereses por cada día de retraso, liquidados a la tasa del 12% efectivo anual.

ARTÍCULO SEGUNDO: ARCHIVAR el cargo formulado en el artículo segundo de la Resolución 51634 del 28 de agosto de 2020, de conformidad con la parte considerativa del presente acto administrativo.

ARTÍCULO TERCERO: Notificar personalmente el contenido de la presente resolución a **CÁMARA DE COMERCIO DE MONTERÍA**, identificada con Nit. 891.080.019-4 a través de su representante legal o quien haga sus veces, en calidad de investigada, entregándole copia de la misma e informándole que contra ella 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 su notificación.

NOTIFÍQUESE Y CÚMPLASE

Dada en Bogotá, D.C., 28 JUNIO DE 2021

El Director de Investigación de Protección de Datos Personales,

CARLOS ENRIQUE
SALAZAR MUÑOZ

Firmado digitalmente por
CARLOS ENRIQUE SALAZAR
MUÑOZ
Fecha: 2021.06.28 11:16:43
-05'00'

CARLOS ENRIQUE SALAZAR MUÑOZ

NOTIFICACIÓN:

Investigada:

Entidad:	CÁMARA DE COMERCIO DE MONTERÍA
Identificación:	Nit. 891.080.019-4
Representante Legal:	FELIX JOSE DE LA CRUZ MANZUR JATTIN
Identificación:	C.C. 19.140.546
Dirección:	Calle 28 No. 4 – 61
Ciudad:	Montería (Córdoba)
Correo electrónico:	administrativa@ccmonteria.org.co