REPUBLICA DE COLOMBIA

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

RESOLUCIÓN NÚMERO 78899 - - DE 2017

(30 NOV. 2017)

VERSIÓN PÚBLICA

"Por la cual se impone una sanción"

Radicación **15-170509**

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 el numeral 5 del artículo 17 del Decreto 4886 de 2011 y,

CONSIDERANDO

PRIMERO: Que 23 de julio de 2015 se presentó ante esta Superintendencia una denuncia por la presunta violación de las normas de protección de datos personales contenidas en la Ley 1581 de 2012, por parte de la copropiedad **INVERSIONES CMR S.A.S.**, por lo que de oficio este Despacho decidió iniciar investigación administrativa con fundamento en los siguientes hechos:

1.1 El 15 de febrero de 2015 el señor [redacted] presentó una queja ante **INVERSIONES CMR S.A.S.** informando el incidente generado a partir del envío de una confirmación a un pedido que el titular hizo a través de la plataforma de domicilios.com, pero cuya confirmación fue enviada al correo electrónico de la señora [redacted], generando que dicha persona se desplazara a casa del señor [redacted], a reclamar sobre la posible tenencia de un celular hurtado y desde el cual ella consideró habían realizado el pedido por la aplicación domicilios.com.

1.2 Que dicha petición fue contestada por **INVERSIONES CMR S.A.S.** el mismo 15 de febrero de 2015 23:52, en la cual le informaban que estaban iniciando el respectivo seguimiento a la situación y que se comunicarían posteriormente.

1.3 El 16 de febrero de 2015 el señor [redacted] reiteró la solicitud de aclaración sobre lo sucedido y una respuesta adecuada a su petición. Dicha comunicación fue contestada mediante escrito el mismo día en el cual le informaban al titular lo siguiente: "(...) verificamos en el sistema y por motivos de actualización de la página ocurrió este error, ya escalamos la situación que es bastante delicada con el área encargada, entendemos su inconformidad y la preocupación de la misma por sus datos personales (...)".

1.4 Que en el mes de abril de 2015, el señor [redacted] le solicitó a la sociedad **INVERSIONES CMR S.A.S.**, lo siguiente:

- ✓ Copia de la **autorización** previa e informada para el manejo de datos personales del Señor [redacted] el cual se encuentra registrado en la plataforma de domicilios. com.
- ✓ Se nos remita las políticas de protección de datos de domicilios
- ✓ Se nos informe que fue lo que ocurrió con la plataforma que le suministró datos personales del Señor [redacted] a un tercero.
- ✓ Las **acciones para solucionar** este inconveniente que afecta de manera grave la privacidad de [redacted]
- ✓ Se nos informe que **medidas de seguridad y metodología** utiliza la aplicación domicilios.com, para corregir los errores de la plataforma, vulnerabilidades, bugs, fallos de configuración, fallos de diseño, fallos en autenticación, en relación con los datos e información de los usuarios

1.5 Que el 16 de abril de 2015 le dan respuesta a su petición, pero el señor [redacted] consideró que fue una respuesta incompleta ya que (i) no le informaron la razón por la cual se dio un "mal tratamiento a los datos personales de [redacted]", (ii) no le entregaron copia de la autorización otorgada por él, (iii) no le indicaron cuál fue la solución dada al error que reconocen sucedió, y (iv) no le demostraron cuáles eran las medidas de seguridad con las que domicilios.com protege los datos personales de los titulares.

SEGUNDO: Que con base en los hechos anotados, a partir de los cuales se advierte la presunta violación de las normas sobre protección de datos personales contenidas en la Ley 1581 de 2012, con la expedición de la Resolución No. 34201 del 31 de marzo de 2016[1], se dio inicio a la presente actuación administrativa y se le formularon cargos a la sociedad **INVERSIONES CMR S.A.S.** por la presunta violación de las disposiciones contenidas en: i) el artículo 9 y 12 y literal b) del artículo 17 de la Ley 1581 de 2012, en concordancia con lo establecido en el artículo 2.2.2.25.2.5 del Decreto 1074 de 2015; ii) el literal d) del artículo 17 de la Ley; iii) los artículos 14 y 15, así como en el literal j) del artículo 17 de la Ley 1581 de 2012; y (iv) el literal n) del artículo 17 de la Ley 1581 de 2012. La mencionada resolución le fue notificada a la investigada para que se pronunciara sobre los hechos materia de investigación y aportara las pruebas que pretendiera hacer valer dentro del referido trámite, con el fin de que ejerciera a cabalidad su derecho de defensa y contradicción. Igualmente se comunicó de la misma actuación al denunciante.

TERCERO: Que la investigada, mediante comunicación del 8 de julio de 2016, presentó escrito de descargos, aduciendo lo siguiente (fls.225 al 401):

3.1 Frente al primer cargo señaló que la Entidad afirma "*erróneamente que INVERSIONES CMR recolecta datos personales desde el momento mismo de la descarga de la aplicación en dispositivos móviles, y durante la realización del registro del pedido de alimentos por parte de los titulares, sin haberles pedido su autorización y sin haber puesto en conocimiento de los mismos el contenido de su política de tratamiento de datos, ni el aviso de privacidad.*", esto basándose en un "*supuesto hallazgo de uno de los funcionarios que lideró la visita de inspección quien afirmó que 'al instalar la aplicación y sin haber hecho pedido alguno, la aplicación DOMICILIOS ya ha recolectado la información de ubicación del titular, y no ha puesto en conocimiento de los titulares la política de tratamiento de datos ni un aviso de privacidad'.*", y que al respecto "*la afirmación es completamente temeraria, pues da por sentado que dicha ubicación es equiparable a un dato personal para cuyo tratamiento se necesita autorización previa, y le da un matiz de incumplimiento al hecho de que la aplicación y la página web permitan ingresar – no almacenar- una dirección o coordenadas en un mapa asociadas a la ubicación de un dispositivo, sin que la persona haya tenido que aceptar los términos y condiciones y la política de privacidad.*"

Que según las definiciones de ley "*el tratamiento limitado a unas coordenadas de ubicación sin incorporar los nombres y apellidos de una persona natural, ni ningún otro dato que permita su individualización, de ninguna manera podría enmarcarse dentro de la definición de dato personal (...)*" y que "*En el caso que nos ocupa, cuando la ubicación inicialmente ingresada se acompaña del nombre del usuario, correo electrónico –entre otros- al momento de realizar un pedido, para que dicha información efectivamente quede almacenada en la base de datos de la Empresa, ese usuario ha tenido que aceptar los términos y condiciones y políticas de privacidad para poder tratar sus datos y concretar el servicio.*".

Por lo que "*el sistema de la Empresa exige que el usuario brinde su consentimiento previo, expreso e informado, sea que esté ingresando a través de la aplicación móvil, página web o a través de su cuenta de Facebook, seleccionando la casilla que dispone expresamente que el usuario ha leído y está de acuerdo con los Términos y condiciones y con las políticas y tratamiento de datos personales.*", "Dicha casilla no se encuentra seleccionada de forma automática, por lo que el usuario conscientemente deberá brindar su autorización inequívoca mediante un 'click' y podrá consultar tanto los términos y condiciones, así como las políticas de tratamiento de datos personales a través de los hipervínculos que allí aparecen"

[1] Obrante carpeta 2 folios 216 al 224.

Afirmó que "*la arquitectura de la base de datos permite que los usuarios de la aplicación 'DOMICILIOS' autoricen de manera inequívoca la utilización de los datos y que el registro de su información se constituya como prueba para demostrar que la Empresa SI posee la autorización dada por los titulares para el tratamiento de su información. En efecto, a pesar de que al momento de la diligencia no había un informe o documento específico en el que se visualizara una casilla determinada a registrar la aceptación de las condiciones y políticas de tratamiento de datos personales, ello de ninguna manera implicaba que INVERSIONES CMR S.A.S. recogía datos personales sin informar al titular, y que además no conservaba copia de la respectiva autorización.*"

Y que "*los responsables del tratamiento están en plena libertad para allegar cualquier medio de prueba que resulte pertinente, conducente e idóneo para demostrar que efectivamente se obtuvo la autorización del usuario, sin que por el simple hecho de no tener una casilla destinada a registrar la aceptación de dichas condiciones implique que 'INVERSIONES CMR S.A.S. no está guardando copia de la respectiva autorización que manifiesta haber recibido de todos los titulares que están registrados en sus bases de datos'.*"

De otro lado, indicó que "*mediante el peritaje técnico realizado se pudo corroborar que cuando un usuario anónimo desatiende un pedido, la aplicación, a través del DEVICE TOKEN o REGISTRATION TOKEN puede enviar una notificación al dispositivo –NO a la persona natural individualmente considerada- a través de un código único que permite conocer la ubicación del sistema. Es muy importante tener en cuenta que estas funcionalidades NO almacenan datos personales. Simplemente almacenan información propia del dispositivo desde el momento en que se ejecuta la aplicación que consiste en un identificador o código de verificación único asociado a la aplicación instalada en el dispositivo. Dicho código puede cambiar si se cambia de dispositivo o si se reinstala la aplicación y por lo tanto, tampoco es equiparable a un dato personal.*"

Así pues, afirmó que "*[e]n cualquier caso, una vez un usuario ha dado su autorización al tratamiento de sus datos por parte de INVERSIONES CMR, el sistema genera un 'log' que representa la constancia de que el usuario aceptó los términos y condiciones y la política de tratamiento de datos, y que por lo tanto, su registro quedó generado para la realización de pedidos. Lo anterior se comprueba con las evidencias 02,03,04,05,06 y 07 que hacen parte integral del Informe Técnico (Prueba 5.2.) (...) dichas evidencias permitieron concluir que: i) que todos los usuarios son informaros(sic) mediante el mecanismo electrónico de aceptación de las políticas de privacidad de los términos y condiciones, y ii) que el registro del usuario de la base de datos de aplicación 'DOMICILIOS' se constituye como la prueba de la autorización para el tratamiento de datos personales, conforme a la ley, ya que sin la autorización no se puede crear, añadir o modificar ningún tipo de dato personal en ningún registro de la Empresa.*"

3.2 Respecto del segundo cargo indicó que "(...) *nunca existió un peligro inminente al que se vieran expuestos los titulares de los datos*", respecto a las medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad de los datos personales aclara que dichas medidas "*(...) deben ser aquellas aplicadas a tiempo, cuando conviene, de forma adecuada, ajustada, conforme a la razón, a las condiciones o necesidades, y de una manera proporcionada y no exagerada. Por lo tanto, no se podrá exigir que los encargados y responsables del tratamiento de las bases de datos implementen medidas de seguridad extremas, innecesarias, exageradas para la protección de los datos.*"

3.2.1 Señaló que respecto de la seguridad interna de la empresa, se implementaron medidas en el hardware y en el software de la empresa y de tecnologías blandas, por lo que se han implementado protecciones en contra de:

- **Amenazas de Software malicioso**

INVERSIONES CMR, en su documento "Política de Seguridad de la Información" posee una norma sobre la protección de virus y software malicioso, donde se exige que todas las estaciones de trabajo tengan instalada y actualizada la herramienta Antivirus 360 Total Security. Así mismo, dicha "Política de Seguridad de la Información" dispone en la sección 5.1.1 normas para el adecuado uso del antivirus y la prevención de softwares o virus maliciosos(Prueba 5.3. pág. 4).

- **Tipos de Computadores**

La mayoría de sistemas operativos utilizados "*para el desarrollo y manejo de información de la aplicación "Domicilios.com" tienen SO de Macintosh (90%).*" Esto agrega "*[u]n nivel extra de seguridad debido que la cuota de computadores con SO Mac en el mundo es solo de un 7% del mercado actual, esto reduce el interés por parte de los hackers en crear "malware" para esta plataforma. Adicionalmente, se tiene configurada la opción de solo instalar aplicaciones de desarrolladores conocidos, las cuales son encontradas en el Mac Store y verificadas por Apple antes de ser publicadas.*" (Prueba 5.3. pág. 5).

- **Topología de red**

"*La red interna en las oficinas de CMR es manejada por separado tanto para la oficina de la Calle 94 como para la oficina de la Calle 93 B..*"(Prueba 5.3. pág. 6)y ambas se encuentran interconectas por una Red Privada Virtual, la cual se encuentra filtrada por los firewalls de ambas redes.

- **Firewall**

"Las oficinas de CMR y del callcenter cuentan con el Firewall Fortinet." (Prueba 5.3. pág. 8)

- **Contramedidas de protección de la información**

"[C]on el fin de proteger a la empresa y al usuario final, INVERSIONES CMR ha implementado una serie de contramedidas para evitar el robo de información y ataque. Entre estas medidas se encuentran:" *1. Sanitización de entradas y salidas de datos, 2. Ataque de Cross-Site Scripting, 3. Ataque de Cross-Site Request Forgery, 4. Peticiones HTTP falsificadas, 5. Protección de credenciales de acceso, 6. Ataques de fuerza bruta, 7. Espionaje de contraseñas, 8. Cookies o variables de sesión persistentes, 9. Servidor de autorización Oauth 1.0a, Autorización de aplicaciones y 11. Encriptación de la llave pública.* (Prueba 5.3. pág. 10).

Y que entre las medidas de tecnologías blandas implementadas se encuentran:

- **Roles y perfiles**

"INVERSIONES CMR cuenta en su Política de Seguridad de Información con una sección dedicada a los roles y responsabilidades, con el objetivo de mantener y detallar el correcto proceder de todos los funcionarios ante las normas prestablecidas."(ver Prueba 5.3. pág. 14).

- **Cláusulas de confidencialidad de los contratos**

INVERSIONES CMR ha mantenido un claro interés por desarrollas las tecnologías blandas, ejemplo de esto son los contratos y/o cláusulas de confidencialidad que ha suscrito con terceros que tienen acceso a la información recolectada por la sociedad. (ver Prueba 5.3. pág. 17).

- **Funcionarios y gestión de datos personales**

"Todos los funcionarios deben tener conocimiento, en mayor o menor grado dependiendo de su posición y qué tanto podría afectar la información de Domicilios.com, de la gestión que se debe dar a los datos personales. Por lo anterior, en el documento de "Políticas de seguridad de la información" Inversiones CMR S.A.S busca mantener la correcta gestión y protección de la información", incluyendo normas que resaltan la importancia y cuidado que debe tener la manipulación de estos datos. (ver Prueba 5.3. pág. 18).

- **Manual de Atención al cliente**

El Manual otorga la suficiente información a los funcionarios sobre la información que puede o no ser recolectada y cómo debe ser el tratamiento de que se le debe dar. (ver Prueba 5.3. pág. 19).

3.2.2 Respecto de la seguridad externa indicó que se encuentran las medidas contratadas por la sociedad e implementadas por terceros, entre las cuales se encuentran:

- **Amazon Web Service (Servicio en la nube)**

"Domicilios.com contrató en Amazon Web Service el servicio de Amazon Elastic Compute Cloud (EC2), el cual es una IaaS que permite el acceso a redes y a equipos virtuales.

El servicio de EC2 funciona junto con Amazon VPC (Virtual Private Cloud) y proporciona seguridad adicional para los recursos informáticos y se destacan las siguientes características:

- *Se encuentra en una VPC con el rango de IP que sea especificado. Esto permite determinar las instancias que se deben exponer en Internet y las que deben permanecer privadas.*
- *Los grupos de seguridad y las listas de control de acceso de red permiten controlar el acceso entrante y saliente de la red.*
- *Permite conectar la infraestructura de IT a los recursos de la VPC mediante conexiones VPN cifradas con los parámetros de seguridad del protocolo de internet."* (ver Prueba 5.3. 19).

(...)

- **Dispositivos móviles soportados**

"La aplicación para celulares de Domicilios.com se encuentra diseñada únicamente para las versiones más recientes de los dispositivos, por lo que únicamente funciona para Android 4.0.3 en adelante y IPhone OS 7 en adelante. La aplicación, por lo tanto, funciona en los celulares que cuenten tanto con las versiones más estables como las actualizaciones y parches de seguridad más recientes." (ver Prueba 5.3. pág. 20).

- **Conexión a la base de datos**

Cada tipo de conexión a la base de datos, es decir, en modo lectura, escritura o desarrollo, tiene reglas y procedimientos definidas para garantizar la protección de la seguridad de la información.(ver Prueba 5.3. pág. 21).

- **Red Segura de Amazon**

En razón de que todo el sistema de INVERSIONES CMR está contenido dentro de una VPN, todos los accesos están determinados únicamente para el servicio web y el acceso de los desarrolladores y administradores y dichos accesos se realizan mediante SSH (*"interprete de ordenes seguro") "o bajo el protocolo HTTPS o en español "protocolo seguro de transferencia de hipertexto""*. este tipo de accesos permite enviar la información de manera encriptada y evitar que un tercero obtenga conocimiento sobre la información enviada. (ver Prueba 5.3. pág. 21).

- **Envío de información a restaurantes**

"Domicilios.com y la plataforma ClickDelivery presentan diferentes tipos de conexiones, las cuales interactúan de cuatro (4) maneras diferentes con los restaurantes a los cuales se transmite el pedido. Para lo anterior se utilizan diferentes niveles de seguridad y varios métodos de transmisión (uno (1) manual, uno (1) semiautomático y dos (2) automáticos)."(ver Prueba 5.3. pág. 22).

- **Sistema de Backup Amazon**

INVERSIONES CMR cuenta con un documento denominado Política de Backups, la cual está diseñada para proteger los datos de la sociedad, asegurando que no se pierdan y que puedan ser recuperados en caso de alguna eventualidad. INVERSIONES CMR cuenta con tres (3) frecuencias diferentes para realizar los backups: respaldos automáticos, respaldos programados y restauración en el tiempo. (ver Prueba 5.3. pág. 23).

3.2.3 Informó que "(...) *el nivel óptimo de administración de la información no es alcanzar un nivel de administración perfecto pero sí un nivel donde los costos y esfuerzos aplicados en esta administración de información no excedan los gastos infringidos por la mala administración de los datos.*", y que "[*e*]*n el caso en concreto, la SIC afirmó que al verse violentada la seguridad de la información de cuatro titulares, se había expuesto de igual forma la seguridad de los datos de cuatrocientos cincuenta mil (450.000) personas más. Sin embargo: '(...) el error generado en la migración ocurrió en la base de datos de Bogotá, que consta de trescientas mil (300.000) cuentas. Adicionalmente, se deben dejar por fuera cincuenta mil (50.000) usuarios de la base de datos de Hello Food, la cual no participó en la migración. Así mismo, el error se presentó en la aplicación móvil de Domicilios.com de la plataforma de Android, la cual presenta 40% de los usuarios totales. En consecuencia, la cantidad de titulares aproximados que supuestamente estuvieron en riesgo durante la migración fue de cien mil (100.000), es decir el 26% de la cantidad total mencionada inicialmente por la SIC'. (ver Prueba 5.3 (...)".*

Complementa lo anterior, indicando que la sociedad *"(...) administra datos de alrededor de cuatrocientos cincuenta mil (450.000) titulares, y de acuerdo con la Resolución se afectó la seguridad de cuatro (4) titulares, dato que representa un porcentaje de: (4/450.000)*100=0,00088%."*, porcentaje que se encuentra *"(...) dentro del nivel óptimo de administración de la información, en tanto sus consecuencias no representan un mayor valor al invertido en administración, esfuerzos y herramientas para la protección de la información y datos personales (...). En consecuencia, no se puede exigir un nivel de absoluta perfección y cero error a la sociedad INVERSIONES CMR en el manejo de sus bases de datos (...)".*

3.3 Respecto del cargo tercero, la sociedad señaló que "(...) el hecho de que INVERSIONES CMR cumpla sí o no con los deberes que ostenta en calidad de Responsable del tratamiento de datos personales, es un supuesto que debe establecerse a partir de un análisis completo y detallado del trámite a través del cual esta Empresa recibe, gestiona y resuelve todo tipo

de PQRs que le son enviada por los titulares de la información. (...) Sin embargo, en el caso presente, la SIC parte del análisis de un total de ocho (8) PQRs que están relacionadas únicamente con la supresión y modificación de datos personales, sin tener en cuenta que INVERSIONES CMR recibe PQRs que versan sobre distintos temas (...) las solicitudes más comunes están relacionadas con los siguientes aspectos:

- **Consultas sobre el estado del pedido (tiempo de entrega y razones por las cuales no ha llegado, entre otras);**
- **Modificaciones al pedido;**
- **Cancelaciones del pedido; y**
- **Quejas con respecto al pedido (lo recibido no coincide con el pedido formulado por el usuario, falta un producto dentro del pedido, se cobró más de lo indicado inicialmente, entre otras).**

Por lo que en la Resolución No. 34201 de 2016 se formuló el cargo tercero partiendo *"(...) del análisis de una mínima parte de la gran variedad y de la totalidad de PQRs que recibe la Empresa. Por lo anterior, es importante remitirse a la gran universalidad de PQRs que existen."*.

Indicó que entre septiembre de 2015 y junio de 2016 se recibieron un total de 13.287 PQRs de las cuales "(...) *la suma de trece mil doscientas setenta y una (13.271) corresponden a solicitudes de modificación de información por parte de los titulares, de las cuales un 99.95% fueron tramitadas y resultadas a tiempo por la Empresa. En cuanto al 0,05% adicional, son trámites que se encuentran en estado nuevo, abierto o pendiente a la fecha de preparación del informe. (...) Por otro lado, durante ese mismo lapso de tiempo se recibieron un total de dieciséis (16) solicitudes de supresión, trece (13) de las cuales fueron eliminadas correspondientemente, mientras que para las tres (3) restantes se presentó el caso de que los titulares de la información continuaron usando la plataforma, razón por la cual los datos de estos titulares hacen parte todavía de la base de datos de la Empresa.*"

Manifestó que la SIC al tomar únicamente ocho (8) solicitudes *"(...) está omitiendo un gran número de PQRs que fueron recibidas, gestionadas y resueltas de acuerdo con los parámetros establecidos en la norma."*

De otro lado, aclaró que la empresa tiene dos tipos de bases de datos:

> (i) la **base de datos de la aplicación,** la cual contiene los datos proporcionados por las personas que se han registrado en Domicilios.com vía web o a través de la aplicación móvil; y
>
> (ii) la **base de datos de marketing,** la cual contiene los datos personales de las personas que reciben *news letter*, es decir, información relacionada con ofertas, productos y servicios.

"(...) *[P]or lo tanto los procesos para llevar a cabo esta supresión, varían dependiendo de que la solicitud se haga respecto a la base de datos de la aplicación, o con respecto a la base de datos de marketing.*"

3.3.1 Respecto de la base de datos de la aplicación indicó que "*[a]l eliminar o suprimir datos personales al interior de la base de datos de la aplicación, estos son suprimidos al mismo tiempo que la cuenta del Usuario se elimina de inmediato. Sin embargo, debe tenerse en cuenta que estos datos son eliminados por completo del registro, pero pueden reposar durante un tiempo en los backups que realiza la Empresa. (...) La política de backups implementada por INVERSIONES CMR consiste en que los datos de un usuario que solicita la supresión permanecen en estos respaldos digitales durante las dos (2) semanas siguientes a la supresión, tiempo después del cual la información es eliminada automáticamente de los servidores.* En efecto, esta policita ha sido diseñada e implementada con el fin de proteger los datos de la empresa, y asegurar que los mismos puedan ser recuperados en caso de que se presente un fallo de infraestructura, una destrucción intencionada de datos, o un desastre". Y que estas políticas y medidas

implementadas para un nivel adecuado de seguridad y proteger la seguridad de la información *"(...) no puede representar bajo ningún entendido una vulneración a los deberes que INVERSIONES CMR ostenta en calidad de Responsable."*

3.3.2 Respecto de la base de datos de marketing señaló que la supresión puede darse *"(...) bien sea i) por solicitud desde el Departamento de Marketing, o ii) por eliminación directa del usuario desde el news letter que recibe en su correo". "En este sentido, (...) aquella información que persiste al interior de esta base de datos se debe a que el usuario ha continuado usando la plataforma, con posterioridad a tramitar la solicitud de supresión."*

Informó que "*En el caso presente, por ejemplo, los usuarios que formularon las quejas #[redacted]; son usuarios que no aparecen en el archivo de usuarios eliminados de la base de datos de marketing, porque estos usuarios hicieron nuevamente uso de la plataforma. Como se ha recalcado, cuando un usuario hace uso de ésta, INVERSIONES CMR requiere de sus datos personales para poder dar trámite y posteriormente perfeccionar la relación de consumo que ha solicitado el usuario. (...) Además, algo que demuestra lo anterior es el hecho de que ninguno de los usuarios que formularon las solicitudes analizadas por parte de la SIC, volvieron a interponer ningún tipo de queja o reclamo ante la Empresa, lo cual implica que se dio el trámite que correspondía para resolverlas.*"

3.4 Respecto del cargo tercero la sociedad indicó que para que exista el deber de informar a la autoridad deben presentarse los dos supuestos de la Ley es decir "*(...) será necesario informar a la autoridad cuando se presenten violaciones a los códigos de seguridad **y** existan riesgos en la administración de la información.*", por lo que "*la sociedad INVERSIONES CMR no cumplió con ninguno de los dos requisitos necesarios para desencadenar el deber indicado en el numeral n).*"

3.4.1 Hay inexistencia de violaciones a los códigos de seguridad puesto que *"(...) la violación a los códigos de seguridad significa que un tercero haya podido acceder a un sistema de información y haya atentado en contra de su seguridad, la cual incluye: disponibilidad, integridad, autenticidad, confidencialidad de los datos. Es por esto que los responsables y encargados del manejo y tratamiento de las bases de datos deben contar con herramientas que les permitan afrontar dichos ataques.*", y que la sociedad cuenta con las siguientes herramientas:

- Labores reactivas
- Herramienta CloudFlare: *funciona como un administrador de solicitudes de internet sobre determinado dominio.* La cual presenta las siguientes acciones:
  - La ubicación de las direcciones IP desde donde se realizan los ataques.
  - Identificación de la zona, región y/o país en el que está asignada la dirección IP.
  - Presentación de resultados al personal que atiende el incidente.
  - Exposición de sugerencias de acciones correctivas sobre las amenazas recibidas en el sistema de Información.
  - Incorporación de filtros de seguridad de acceso a los DNS indicados por el administrador de la plataforma. (Prueba 5.5.)

Adicionalmente, indicó que *"[s]in perjuicio de la implementación de las acciones de mitigación, será necesario que respecto de ataques DoS (Ataques de Denegación de Servicios), los cuales son eventos que atentan contra la seguridad de la información de INVERSIONES CMR, toda vez que altera la disponibilidad de un sistema de información, la sociedad INVERSIONES CMR informe a la SIC sobre dicha eventualidad en tanto cumple con lo exigido por el literal n). Ejemplo de lo anterior es el informe con radicado No. 16-180684, donde se reportó el incidente menor ocurrido los días 17 y 18 de junio de 2016 (...). En conclusión, la sociedad INVERSIONES CMR no debió informar a la SIC la existencia de una violación a los códigos de seguridad, en tanto no ocurrió en el tiempo determinado por la SIC."*

3.4.2 Hay inexistencia de riesgos en la administración de la información de los titulares puesto que *"[d]e conformidad con lo expuesto en las consideraciones al Cargo Dos, se concluyó*

que el porcentaje de error que existió durante el lapso de tiempo especificado por l(sic) SIC fue del 0.8% de una muestra de 450.000, el cual no logra constituir siquiera el 1% y que por lo tanto este porcentaje no se encontraba dentro del nivel óptimo de administración de la información, en tanto sus consecuencias no representan un mayor valor al invertido en administración, esfuerzos y herramientas para la protección de la información y datos personales (...)".

"En conclusión, es evidente que INVERSIONES CMR nunca expuso a un riesgo en la administración de la información de los cuatrocientos cincuenta mil titulares sobre los cuales posee datos y tampoco fue objeto de una violación a los códigos de seguridad por lo que no debió informar a la SIC, de la manera que lo indica el numeral n) del artículo 17 de la Ley 1581 de 2012, por lo que el cargo no procede."

3.5 Aclaró que la sociedad *"(...) no trata ni administra de ninguna manera datos sensibles, en tanto no contienen información intima o que pueda ser utilizada como razón de discriminación en contra de sus titulares. Lo anterior se expone con la intención de generar una proporcionalidad en el deber de seguridad que debe ser implementado respecto de la por INVERSIONES CMR."*

CUARTO: Que el 9 de septiembre de 2016 mediante comunicación de radicado15-170509--00015, la sociedad investigada presentó memorial de alcance señalando lo siguiente:

4.1 Que mediante radicado No. 16-180684 se informó a la Superintendencia de Industria y Comercio *"acerca de la materialización de una violación a los códigos de seguridad y la existencia de un riesgo en la administración de la información de los titulares del aplicativo 'domicilios.com' de los sistemas operativos Android e iOS, perteneciente a la infraestructura tecnológica de Inversiones CMR S.A.S., dando alcance al deber consagrado en el literal n) del artículo 17 de la Ley 1581 de 2012"* y que el 29 de agosto de 2016 se otorgó respuesta archivando el expediente por no tener mérito. *"Respecto de la anterior decisión, se realizan las siguientes declaraciones:*

1. De acuerdo a la SIC, sólo se debe informar en el momento en que *se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.* Es decir, la SIC entiende que el deber de informar se da en el momento de cumplir con ambos requisitos; en el mismo sentido en que se argumentó el cargo cuarto de los descargos.
2. De acuerdo a la SIC, una afectación no es lo mismo que una fuga de información o acceso no autorizado a los datos personales.
3. Una afectación no es causal para activar el deber del literal *n) del artículo 17 de la Ley 1581 de 2012.*
4. La SIC, en el expediente No. 16 180684, reitera lo dicho en la Circular Externa número 002 y en las Guías de Responsabilidad Demostrada (Accountability), donde los incidentes de seguridad se definen como:

> *"(ii) Incidentes de Seguridad. Se refiere a la violación de los códigos de seguridad o la pérdida. Robo y/o acceso no autorizado de información de una base de datos administrada por el Responsable del Tratamiento o por su Encargado"*
>
> *"...se refieren a cualquier evento en los sistemas de información o bases de datos manuales o sistematizadas, que atente contra la seguridad de las datos personales en ellas almacenados..."*

De modo que, la violación a los códigos de seguridad significa que un tercero haya podido acceder a un sistema de información y haya atentado en contra de su seguridad, la cual incluye: disponibilidad, integridad, autenticidad, confidencialidad de los datos.

5. INVERSIONES CMR nunca expuso a un riesgo en la administración de la información de los cuatrocientos cincuenta mil titulares sobre los cuales posee datos y tampoco fue objeto de una violación a los códigos de seguridad por lo que no debió informar a la SIC, de la manera que lo indica el numeral n) del artículo 17° de la Ley 1581 de 2012, por lo que el cargo no procede.

4.2 Solicitó que *"(...) la respuesta otorgada por la SIC, dentro del expediente No. 16 180684 sea tenida en cuenta en la valoración de los Descargos, dentro del presente proceso. Así mismo, se solicita que la SIC procesa a declarar mediante acto administrativo debidamente motivado que INVERSIONES CMR S.A.S queda exonerado y absuelto de toda responsabilidad por supuesta violación de normas de Protección de Datos Personales y en consecuencias(sic) de todos los cargos formulados en la Resolución, de conformidad con los argumentos y pruebas allegadas, y por lo mismo, se ordene el archivo del expediente."*

QUINTO: Que mediante Resolución No. 82197 del 28 de noviembre de 2016, se negaron unas pruebas solicitadas, se incorporaron con el valor legal que les corresponda, todos los documentos obrantes en el expediente 15-170509 de folios 1 al 400, inclusive los aportados por la investigada, junto con los folios 1 al 34 del cuaderno de reserva, y se corrió traslado a la investigada para que rindiera los alegatos respectivos.

SEXTO: Que mediante Resolución No. 83600 del 2 de diciembre de 2016 se corrigió un error formal contenido en la Resolución No. 821987 del 28 de noviembre de 2016 aclarando el número de radicado de la Resolución, dicha corrección no afecta el sentido material de la decisión ni revive términos legales.

SÉPTIMO: Que de acuerdo con comunicación remitida por la investigada el 14 de diciembre de 2016, mediante la cual dio respuesta al traslado para presentar alegatos de conclusión remitido por este Despacho, el apoderado especial de la sociedad **INVERSIONES CMR S.A.S** manifestando lo siguiente (fls.419 al 435):

7.1 Reiteró todo lo manifestado en el escrito de descargos y señaló que "(...) *en concordancia con las pruebas aportadas dentro del proceso, el Despacho deberá concluir que los cargos propuestos no prosperan, toda vez que los hechos que los fundamentan fueron controvertidos y desestimados en los t[términos(sic) ampliamente expuestos en el escrito de descargos y en el presente documentos(sic) de alegatos de conclusión."*

7.2 Solicitó a esta Superintendencia que *"(...) proceda a declarar mediante acto administrativo debidamente motivado que INVERSIONES CMR S.A.S. queda exonerado y absuelto de toda responsabilidad por supuesta violación de normas de Protección de Datos Personales y en consecuencia de todos los cargos formulados en la Resolución, de conformidad con los argumentos y pruebas allegadas, y por lo mismo, se ordene el archivo del expediente de conformidad con lo dispuesto en el artículo 49 de la Ley 1437 de 2011 y en concordancia con el principio de congruencia que rige esta actuación administrativa."*

OCTAVO: Competencia de la Superintendencia de Industria y Comercio

El artículo 19 de la Ley 1581de 2012, establece la función de vigilancia que le corresponde a la Superintendencia de Industria y Comercio para garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la ley.

NOVENO: Análisis del caso

9.1 Adecuación típica

La Corte Constitucional mediante sentencia C-748 de 2011[2], estableció lo siguiente en relación con el principio de tipicidad en el derecho administrativo sancionatorio:

> *"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".*

Atendiendo los parámetros señalados por la citada jurisprudencia, para el caso específico se tiene que:

---

[2] Corte Constitucional, Magistrado Ponente Jorge Ignacio Pretelt Chaljub, seis (6) de octubre de dos mil once (2011).

(i) El artículo 17 de la Ley 1581 de 2012 establece los deberes que les asisten a los responsables del tratamiento respecto del manejo de los datos personales de los titulares. El incumplimiento de tales requisitos dará lugar a la aplicación de las sanciones definidas específicamente en el artículo 23 de la Ley 1581 de 2012.

(ii) De conformidad con los hechos alegados por el reclamante y el acervo probatorio que obra en el expediente, se puede establecer que la conducta desplegada por la investigada se concreta en la posible vulneración de las disposiciones contenidas en: i) el artículo 9 y 12 y literal b) del artículo 17 de la Ley 1581 de 2012, en concordancia con lo establecido en el artículo 2.2.2.25.2.5 del Decreto 1074 de 2015; ii) el literal d) del artículo 17 de la Ley; iii) los artículos 14 y 15, así como en el literal j) del artículo 17 de la Ley 1581 de 2012; y (iv) el literal n) del artículo 17 de la Ley 1581 de 2012

En ese orden de ideas, corresponde a este Despacho establecer si la conducta desplegada por la investigada dará lugar o no a la imposición de una sanción para lo cual se deberán tener en cuenta los hechos narrados por el reclamante, así como las razones de hecho y de derecho aducidas por la investigada en los escritos de descargos y alegatos de conclusión, y el conjunto de pruebas allegadas al expediente.

9.2 Valoración probatoria y conclusiones

A continuación se realizará un análisis de cada uno de los cargos imputados a la investigada en la presente actuación, así como el acervo probatorio recaudado, para en cada caso establecer si se presentó una infracción al Régimen de Protección de Datos Personales.

9.2.1 Respecto del deber de solicitar y conservar copia de la autorización previa e informar al titular las finalidades de la recolección

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 fundamentales como el de intimidad y el libre desarrollo de la personalidad. En efecto, el ser humano goza de la garantía de determinar qué datos quiere sean conocidos y tiene el derecho a determinar lo que podría denominarse su 'imagen informática'"*[3].

Por lo anterior, se concluye que sin la autorización previa e informada del titular, los datos personales no podrán ser registrados, divulgados, ni tratados. Sin embargo, tal prohibición no es absoluta pues la Ley 1581 de 2012 en su artículo 10 establece los casos en los que no es necesario contar con la autorización por parte del titular, entre los cuales se encuentran los datos de naturaleza pública[4].

---

[3] Ver en: Corte Constitucional Sentencia C-748 del 6 de octubre de 2011 MP. Jorge Ignacio Pretelt Chaljub.

[4] *"**Artículo 10. Casos en que no se necesita la autorización.** La autorización del Titular no será necesaria cuando se trate de:*
a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;
b) Datos de naturaleza pública;
c) Casos de urgencia médica o sanitaria;
d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;
e) Datos relacionados con el Registro Civil de las Personas.

El artículo 4 de la Ley 1581 de 2012, contempla los principios para el tratamiento de datos personales, entre los cuales se encuentra el principio de finalidad que señala que *"(e)l Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular*". Sobre esto, la Honorable Corte Constitucional en sentencia C-748 de 2011, señaló que en virtud del principio de finalidad los datos personales deben ser procesados con un propósito específico y explicito, razón por la cual se impone el deber de informar clara, suficiente y previamente al titular acerca de la finalidad de la información suministrada, prohibiendo así la recopilación de datos sin la especificación clara acerca de su finalidad.

Los principios rectores, que para el cargo primero son el de libertad y finalidad, deben confluir en cuanto a su aplicación con los deberes y derechos contenidos en la Ley 1581 de 2012, específicamente para el cargo es relevante mencionar el deber consagrado en el literal b) de solicitar y conservar copia de la respectiva autorización otorgada por el titular y en el literal c) de informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten en virtud de la autorización.

Adicionalmente, el artículo 12 de la misma Ley, señala que el responsable debe informar clara y expresamente al titular: (i) el tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo; (ii) 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; (iii) Los derechos que le asisten como Titular; (iv) La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.

En virtud de lo expuesto, es importante aclarar que el consentimiento es un elemento **esencial** en el manejo de la administración de los datos, y que el mismo debe ser calificado, por cuanto debe ser previo, expreso e **informado**, así pues, el titular antes de expresar su consentimiento debe conocer las finalidades para las cuales serán tratados sus datos, con el fin de autorizar su conservación, uso y circulación según lo informado por el responsable del tratamiento, y así poder hacer uso de la libertad frente al poder informático y la autodeterminación informática.

En este mismo sentido, la Corte Constitucional señaló lo siguiente:

> *"La libertad en la administración de datos personales significa que el sujeto concernido mantenga, en todo momento, las facultades de conocimiento, actualización y rectificación de la información personal contenida en las bases de datos. Si ello es así, es evidente que la libertad del individuo ante el poder informático se concreta, entre otros aspectos, en la posibilidad de controlar la información personal que sobre sí reposa en las bases de datos, competencia que está supeditada a que exprese su consentimiento para la incorporación de la información en el banco de datos o archivo correspondiente.* ***Este ejercicio de la libertad en los procesos informáticos, a juicio de la Corte, se concreta en la exigencia de autorización previa, expresa y suficiente por parte del titular de la información, requisito predicable de los actos de administración de datos personales de contenido comercial y crediticio. La eliminación del consentimiento del titular, adicionalmente, genera una desnaturalización del dato financiero, comercial y crediticio, que viola el derecho fundamental al hábeas data, en tanto restringe injustificadamente la autodeterminación del sujeto respecto de su información personal. Para la Constitución, la libertad del sujeto concernido significa que la administración de datos personales no pueda realizarse a sus espaldas, sino que debe tratarse de un proceso transparente, en que en todo momento y lugar pueda conocer en dónde está su información personal, para qué propósitos ha sido recolectada y qué mecanismos tiene a su disposición para su actualización y rectificación. La eliminación de la autorización previa, expresa y suficiente para la incorporación del dato en los archivos y bancos de datos administrados por los operadores permite, en últimas, la ejecución de actos ocultos de acopio, tratamiento y divulgación de información, operaciones del todo incompatibles con los derechos y garantías propios del hábeas data.*** *(Resaltado fuera del texto)"*[5]

Así mismo, el artículo 2.2.2.25.2.5 del Decreto 1074 de 2015 fue claro en indicar lo siguiente:

> *"**Artículo 2.2.2.25.2.5. 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." (subrayado fuera del texto"*

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

[5] Ver en: Corte Constitucional Sentencia C-748 del 6 de octubre de 2011 MP. Jorge Ignacio Pretelt Chaljub.

De la visita de inspección y una vez analizada la documentación recolectada y aportada por la sociedad se evidenciaron los siguientes hallazgos:

Se tomó una muestra aleatoria de ocho (8) Titulares que habían presentado peticiones en ejercicio del derecho de *habeas data*, con el fin de verificar la manera en que la sociedad inspeccionada solicita y conserva la copia de la autorización otorgada para el tratamiento de datos personales. Adicionalmente, se solicitó copia de la autorización otorgada por los titulares [redacted].

La sociedad no remitió copia de la manifestación expresa mediante la cual el titular autoriza el tratamiento de sus datos personales, con base en que "*la plataforma de propiedad de INVERSIONES CMR S.A.S no admite el registro de usuarios nuevos hasta tanto éstos no otorguen su autorización para el trámite de sus datos personales*".

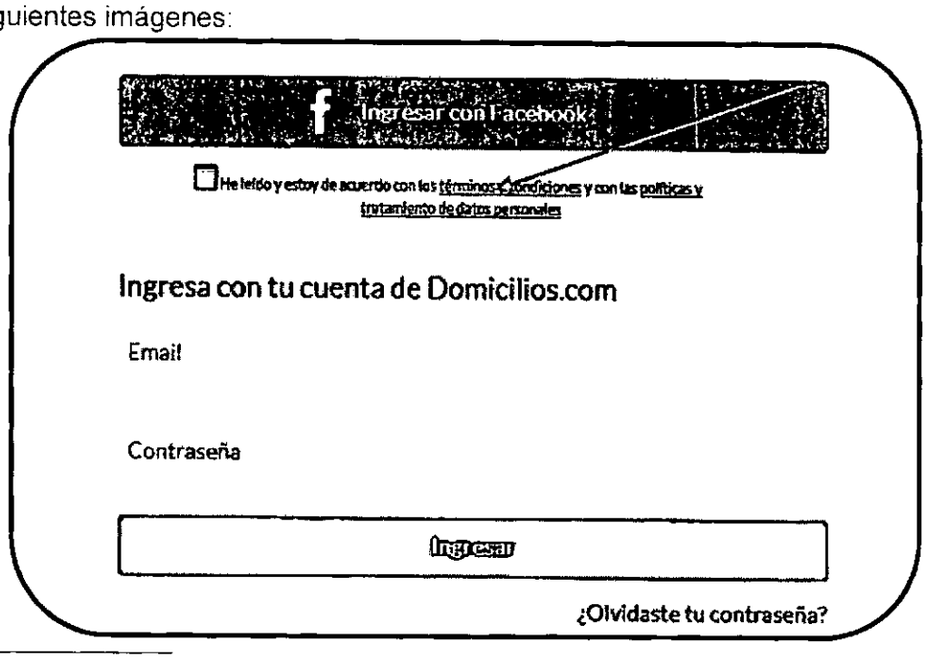
Respecto a los Titulares [redacted] y [redacted], en desarrollo de la visita de inspección se evidenció que los datos personales de los mismos existen en la base de datos de **INVERSIONES CMR S.A.S**, y como prueba de ello, mediante la captura del "*log*"[6] de dicha información se realiza una preservación de información donde se evidenció que en el esquema de la base de datos (tipología de la base) de **INVERSIONES CMR S.A.S**, no tiene destinado un campo para el registro de la aceptación de los "Términos y Condiciones" y política de tratamiento de datos personales.

De otra parte, la sociedad investigada informó que "*no se allegaron todos los archivos ('logs') puesto que por la antigüedad de las cuentas no es fácil acceder a ellos en el sistema y a la fecha ello no se ha podido lograr*".

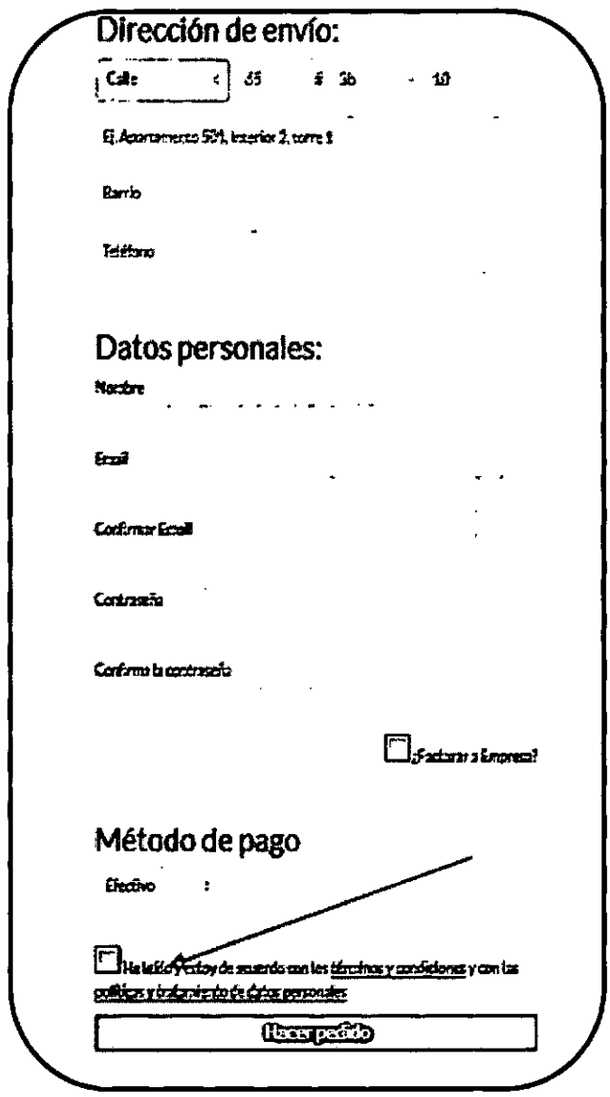
Así pues, se puede concluir que en la visita de inspección y una vez revisado el material aportado y recolectado, se encontró que la sociedad i) está atando la solicitud de autorización al registro de nuevos usuarios y ii) no cuenta con los archivos "*logs*" de todas las cuentas registradas.

Frente a lo mencionado, la sociedad indicó en escrito de descargos y alegatos de conclusión que: i) *"(...) la plataforma de propiedad de INVERSIONES CMR no admite la realización de pedido alguno ni el registro de usuarios nuevos hasta tanto éstos no otorguen su autorización para el tratamiento de sus datos personales. (...) el sistema de la Empresa exige que el usuario brinde su consentimiento previo, expreso e informado, sea que éste ingresando a través de la aplicación móvil, página web o a través de su cuenta de Facebook, seleccionando la casilla que dispone expresamente que el usuario ha leído y está de acuerdo con los Términos y condiciones y con las políticas y tratamiento de datos personales".* (Cuaderno 2 fl.227)

Aporta las siguientes imágenes:



[6] Anglicismo derivado de las traducciones del inglés en la jerga informática, cuya traducción literal es Bitácora. En sistemas de información, un log es un registro de actividad de un sistema, que generalmente se guarda en un archivo de texto, al que se le van añadiendo líneas a medida que se realizan acciones sobre el sistema.



La sociedad investigada afirma que "*Si la persona no aceptara que está de acuerdo con los términos y condiciones y con las políticas de tratamiento de sus datos, no se crea registro alguno del usuario en la base de datos, simplemente NO existe*. Así las cosas, los registros de información de los titulares previamente allegados en el marco de la investigación, así como el Informe Técnico que se anexa como prueba 5.2. junto con este escrito, se constituyen como prueba pertinente, conducente e idónea para demostrar que efectivamente se cuenta con su autorización para el tratamiento de sus datos (...)" (fl.228).

Teniendo en cuenta lo expuesto anteriormente, así como las pruebas obrantes en el expediente, los hallazgos y los escritos de descargos y alegatos de conclusión se encuentra demostrado que i) la sociedad **INVERSIONES CMR S.A.S** recolecta datos personales a través de la aplicación móvil, página web y a través de la cuenta de Facebook y ii) que a través de estos medios la sociedad tiene implementada una casilla mediante la cual, a través de un "*click*" el titular acepta que "*He leído y estoy de acuerdo con los términos y condiciones y con las políticas y tratamiento de datos personales*" (Cuaderno 2 fls.227 y 228).

Ahora bien, la Ley 1581 de 2012 en su literal b) establece no solo el deber de solicitar la autorización previa y expresa del titular sino también el de conservar copia de la autorización, así mismo, el artículo 9 de la norma en mención establece que *"(...) 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.*".

Por lo anterior, es claro el cumplimiento del deber objeto de estudio no se limita únicamente a solicitar la autorización sino que el mismo se extiende a conservar copia de la misma en un medio que permita su consulta posteriormente.

Frente a la copia de la autorización, encontramos que la sociedad a lo largo de la investigación administrativa señala dos situaciones: (i) que mediante la fecha de creación en el sistema de la cuenta de los usuarios se tiene la autorización del mismo pues el sistema no permite realizar pedidos a través de la plataforma hasta tanto no se otorgue la autorización y (ii) mediante un "log" se presenta la constancia de que el usuario aceptó los términos y condiciones y la política de tratamiento de datos.

Al solicitar la autorización de ocho (8) titulares seleccionados aleatoriamente, la sociedad aportó la siguiente relación de datos donde se evidencia la fecha de creación de los mismos (fl.27):

#	ID en visita	ID en Respuesta del 20-11-2015	Nombre	Correo	Fecha de creación
1	[redacted]				12/12/2014
2					08/06/2014
3					03/09/2013
4					25/09/2013
5					*
6					*
7					26/09/2014
8					30/08/2013

*Manifestaron no contar con dicha información por haberle dado trámite a la solicitud de eliminación.

Al respecto, la sociedad señala que *"[e]n cualquier caso, una vez un usuario ha dado su autorización al tratamiento de sus datos por parte de INVERSIONES CMR, el sistema genera un "log" que representa la constancia de que el usuario aceptó los términos y condiciones y la política de tratamiento de datos, y que por lo tanto, su registro quedó generado para la realización de pedidos*" (Cuaderno 2 fl.229).

Analizados los "*logs*" aportados por la investigada obrantes de folios 200 a 203 encontramos que los mismos sólo indican la fecha de creación del usuario, que según la sociedad sucede sólo si el titular acepta los términos y condiciones y tratamiento de datos personales, sin embargo, i) la sociedad no demuestra ni es posible saber si así funcionaba el registro cuando se crearon los usuarios de quienes no presentó evidencia de la autorización, más aun cuando la creación de dichos usuarios es previa a cuando sucedieron los hechos el 15 de febrero de 2015, y ii) en los "*logs*" aportados no se evidencia que existía la validación del "*check*" en la casilla para aceptar los términos y condiciones y tratamiento de datos personales.

Por lo anterior, no es posible determinar que al momento de crear la cuenta de los titulares seleccionados aleatoriamente los mismos autorizaron a la sociedad **INVERSIONES CMR S.A.S** para realizar el tratamiento de sus datos personales, y en consecuencia no se demostró que respecto de los titulares seleccionados se cumpliera con el deber de informar.

En virtud de lo expuesto, esta Dirección encuentra que la sociedad investigada **INVERSIONES CMR S.A.S** no demostró cumplir con los deberes que ostenta en su calidad de Responsable de la información contemplados en el artículo 9 y 12 y los literales b) y c) del artículo 17 de la Ley 1581 de 2012, en concordancia con lo establecido en el artículo 2.2.2.25.2.5 del Decreto 1074 de 2015, frente al tratamiento de datos de los titulares seleccionados aleatoriamente, razón por la cual se impondrá la correspondiente sanción.

9.2.2 Respecto del deber de conservar la información bajo las condiciones de seguridad necesarias que sean necesarias para impedir el acceso no autorizado

Bajo los postulados que gobiernan la disposición contenida en el literal d) del artículo 17 de la Ley1581 de 2012, es evidente que para que se pueda extraer un juicio de responsabilidad como consecuencia de la infracción a este deber, debe demostrarse que la información personal de los Titulares fue accedida por terceros no autorizados, rompiendo con los principios de circulación restringida y de seguridad de la información.

Por su parte, teniendo en cuenta el artículo 15 de la Constitución Política de Colombia, en concordancia con los principios rectores de seguridad y de confidencialidad, se tiene que como una extensión de los mismos, el legislador concibió en el literal d) del artículo 17 de la Ley Estatutaria de Protección de Datos Personales, como deber de los Responsables en el Tratamiento de datos, la conservación de la información con todas las medidas de seguridad que sean necesarias con el fin de no poner en riesgo los datos personales de los Titulares.

Así pues, el Responsable deberá tener en cuenta tanto el volumen de la base de datos a la que realiza Tratamiento, como la naturaleza de los datos que trata, haciendo que dichas medidas o controles de seguridad sean directamente proporcionales a los datos alojados.

De esta manera el legislador dispuso, entre otros, como principios rectores del Tratamiento y la administración de los datos personales el principio de seguridad y de confidencialidad que a la luz del artículo 4 de la Ley 1581 de 2012 disponen lo siguiente:

> *"(...)*
>
> ***Principio de acceso y circulación restringida:*** *El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley;*
>
> *Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley;*
>
> *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;*
>
> *(...)".*

Al respecto la Corte Constitucional ha relacionado este deber con el principio de seguridad, manifestando que la *"(...) información sujeta a tratamiento por el responsable o encargado, 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"*[7].

Como se advierte, tanto el principio de acceso y circulación restringida como el de seguridad deben ser cumplidos por los Responsables y Encargados de información para garantizar el derecho de *hábeas 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.

Ahora bien, retomando el caso bajo estudio, se encuentra que el denunciante afirma que la sociedad **INVERSIONES CMR S.A.S** divulgó a terceros no autorizados su información personal, específicamente la confirmación de su pedido mediante correo electrónico a la señora [redacted] generando que dicha persona se desplazara a casa del señor [redacted] a reclamar la posible tenencia de un celular hurtado y desde el cual ella consideró que habían realizado el pedido por la aplicación domicilios.com.

---

[7] Ver en: Corte Constitucional Sentencia C-748 del 6 de octubre de 2011 MP. Jorge Ignacio Pretelt Chaljub.

Al respecto, comenzará la Dirección tomando como base las pruebas recaudadas por el Laboratorio de Informática Forense de la Superintendencia de Industria y Comercio, el cual obtuvo una serie de hallazgos al realizar una verificación técnica del proceso de migración de bases de datos de **INVERSIONES CMR S.A.S** adelantado desde diciembre de 2014, en las cuales se unificaron bases de titulares registrados desde Cali, Medellín, y Bogotá, así como la base de datos de HelloFood, donde se recolectó evidencia digital pertinente, así como testimonios y pruebas las cuales fueron consignadas en el Acta de Visita de Inspección suscrita el 28 de octubre de 2015.

Dentro de los hallazgos relevantes al estudio del deber se evidencia que en el proceso de migración se presentó una falla que generó el envío errado de datos personales en las confirmaciones de pedidos a usuarios que no los habían realizado. Lo anterior se soporta en lo confesado por el Gerente Técnico y de Mercadeo de la sociedad investigada quien reconoció que existió un "*error Tecnológico*" [8] el cual se materializó en el envío de comunicaciones de confirmación de pedido con el envío de los datos personales de los clientes: nombre, dirección de domicilio y teléfono, adicionalmente, lo confesado se soporta en la verificación de las solicitudes seleccionadas aleatoriamente en la diligencia de visita de inspección, de las cuales se resalta lo siguiente:

1. [redacted] petición No. [redacted] presentada el 8 de julio de 2015, a través de la cual se quejó por recibir en reiteradas ocasiones confirmaciones de pedidos no solicitados, señalando que *"(...) no me envíen más de estos email porque no me corresponden a mi persona"*[9].

2. [redacted] petición No[redacted] presentada el 27 de julio de 2015 y reitera el 7 de agosto del año en mención, a través de la cual manifestó lo siguiente: "*NO QUIERO VERIFICAR UN PEDIDO. QUIERO QUE ELIMINEN DEFINITIVAMENTE MIS DATOS DE SU DIRECTORIO*"[10].

3. [redacted] petición No. [redacted] presentada el 6 de junio de 2015, a través de la cual afirmó "*nuevamente me están enviando correos de domicilios que no he pedido. Por favor verifiquen, revisen y coordinen sus bases de datos*"[11].

4. [redacted] petición No. [redacted] presentada el 15 de febrero de 2015, a través de la cual solicitó "*Ruego por favor inicien una explicación técnica de esta orden pues aparece simultáneamente en correo de otra persona, con información personal del suscrito, de igual manera preocupa que dicha información este(sic) llegando a más personas, poniendo en alto riesgo al titular (...) al proporcionar información privada.*"[12].

Por lo cual se encuentra demostrado que en estos casos específicos la información personal contenida en las bases de datos de la sociedad fue accedida por terceros no autorizados quienes recibían correos de confirmación de pedidos con datos personales de titulares.

Al respecto y de manera posterior, haciendo uso del derecho de defensa que le asiste a los investigados en el proceso administrativo sancionatorio la sociedad INVERSIONES CMR S.A.S., mediante el escrito de descargos, presentó los argumentos que, en su consideración, demuestran que no trasgredió el deber expuesto en el literal d) del artículo 17 de la Ley 1581 de 2012. Dichos argumentos se sintetizan en lo siguiente: "*(...) nunca existió un peligro inminente al que se vieran expuestos los titulares de los datos*" (Cuaderno 2 reverso fl.229), que *"(...) no se podrá exigir que los encargados y responsables el tratamiento de las bases de datos implementen medidas de seguridad extremas, innecesarias, exageradas para la protección de los datos*" (Cuaderno 2 fl.230) y que "(...) *ha implementado diferentes tipos de políticas y herramientas para garantizar la correcta gestión de la seguridad de los datos personales y sensibles (...) en la medida que la Empresa ha*

---

[8] Manifestación hecha por el señor [redacted], Gerente de Tecnología en visita del 27 y 28 de octubre de 2015.

[9] Carpeta Reservada CD fl.1 Ubicación: E:\DOMICILIOS.COM\DOMICILIOS.COM\DOMICILIOS.COM_INFORMACION_DB\DOMICILIOS.COM_INFORMACION_PQR\DOMICILIOS.COM_INFORMACION_PQR\pqr\Solicitud y respuesta 218806.pdf

[10] Carpeta Reservada CD fl.1 Ubicación: E:\DOMICILIOS.COM\DOMICILIOS.COM\DOMICILIOS.COM_INFORMACION_DB\DOMICILIOS.COM_INFORMACION_PQR\DOMICILIOS.COM_INFORMACION_PQR\pqr\solicitud ticket 227010.pdf

11 Carpeta 1 folios 51 al 54.

12 Carpeta 1 folio 13.

almacenado los datos personales bajo las medidas técnicas, humanas y administrativas adecuadas para garantizar la seguridad de la información y evitar su pérdida, acceso o uso no autorizado." (Cuaderno 2 reverso fl.232).

De otro lado, advierte que *"(...) INVERSIONES CMR administra datos de alrededor de cuatrocientos cincuenta mil (450.000) titulares, y de acuerdo con la Resolución se afectó la seguridad de cuatro (4) titulares, dato que representa un porcentaje de: (4/450.000)*100=0,00088%. (....) Es decir, el porcentaje de error que existió durante este lapso de tiempo fue del 0.00088% de una muestra de 450.000, el cual no logra constituir siquiera el 0,001%. Este porcentaje por lo tanto, se encuentra dentro del nivel óptimo de administración de la información, en tanto sus consecuencias no representan un mayor valor al invertido en administración, esfuerzos y herramientas para la protección de la información y datos personales (...)"* (Cuaderno 2 fl.234).

Al respecto, frente a la afirmación según la cual nunca existió un peligro inminente al que se vieran expuestos los datos de los titulares, esta Dirección aclara que tal como lo afirma claramente la sociedad investigada tanto en la visita de inspección como a través de la presente actuación, se realizó el envío de correos de confirmación de pedidos que contienen datos personales a terceros no autorizados, permitiendo el acceso de terceros consecuencia de un "*error tecnológico*" generado en la migración de los datos en el proceso de unificación.

En adición a lo anterior, se probó que no obstante la sociedad **INVERSIONES CMR S.A.S.** conoció el acceso no autorizado por parte de terceros, esto a través de correos electrónicos solicitando el no envío de confirmaciones de pedidos los cuales no han sido solicitados, no implementó medidas técnicas y metodológicas necesarias para evitar que continuara esta difusión de información.

Es necesario señalar que tanto los Responsables como los Encargados del tratamiento deben identificar y determinar los riesgos asociados al tratamiento de datos personales que realizan dependiendo de la estructura organizacional, sus procesos y procedimientos internos asociados al tratamiento de datos personales, la cantidad de bases de datos y el tipo de datos personales tratados por la empresa para establecer las medidas o controles que permitan la identificación, medición control y monitoreo de los hechos o situaciones que puedan incidir en la debida administración del riesgo al que están expuestos los datos.

Teniendo en cuenta que se encuentra demostrado que se realizó una difusión no autorizada de los datos personales a través de correos de confirmación de pedidos, esta Dirección encuentra que las medidas de seguridad implementadas por la sociedad investigada no fueron las necesarias para evitar que sucediera el riesgo asociado al tratamiento, así como las medidas correctivas no fueron tomadas a tiempo para impedir que el acceso no autorizado de los datos personales continuara sucediendo.

Así las cosas, revisado el material probatorio obrante en el expediente y los hallazgos encontrados en la visita de inspección esta Dirección no evidencia un plan de migración de datos, donde se pueda comprobar que la sociedad investigada tomó las medidas necesarias para evitar el cruce de identificadores (Id) que por ciudad pudiesen quedar repetidos que según señala la sociedad, fue lo que sucedió. Adicionalmente, no existe un plan de pruebas una vez realizada la migración e integración de datos que demostrara que se tomaron las medidas técnicas y metodológicas necesarias para evitar la difusión y uso no autorizado evidenciado.

Ahora bien, respecto a la muestra tomada en la visita de inspección de ocho (8) titulares respecto de cuatrocientos cincuenta mil (450.000), si bien, la muestra es insignificante frente al monto total de titulares, evidentemente se presentó una falla en salvaguardar la confidencialidad de los datos personales que fueron expuestos a terceros no interesados.

Si bien, el informe de seguridad contratado con la firma Berkeley Research Group (Cuaderno 2 fls.268 al 293) relaciona una serie de buenas prácticas implementadas en la sociedad investigada, así como la descripción del flujo de información generado en los distintos procesos, sin embargo, no se evidencia el flujo ni los controles implementados en el momento en que se envían los correos para confirmar el pedido, que fue exactamente donde se generó el error y por lo tanto la queja del denunciante. En la misma medida, tanto en la fecha de la visita, como en las pruebas aportadas, no fueron relacionadas concretamente las medidas técnicas, humanas y/o administrativas

tomadas para corregir específicamente el error presentado, a pesar de que muestran buenas prácticas en el proceso de desarrollo (Carpeta 2 fl.330), no es claro que las mismas se hayan tomado para contener el incidente presentado.

Adicionalmente, esta Dirección encuentra que estas buenas prácticas señaladas por la investigada para demostrar que no trasgredió el deber estudiado, previenen otro tipo de incidentes y ataques, es decir las mismas se establecen para evitar ataques, fuga de información y accesos no autorizados **premeditados**, pero no corrigen el error presentado causante del incidente objeto de la presente investigación.

En virtud de lo expuesto, esta Dirección encuentra que respecto a los datos personales de ocho (8) titulares la sociedad no cumplió el deber de conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, y aunque la sociedad se enteró de este acceso no autorizado por parte de terceros a través de las quejas presentadas por los titulares señalados, no tomó medidas a tiempo respecto a este acceso no autorizados, así como tampoco tomo medidas a tiempo para corregir esta fuga de información con el fin de que no continuara sucediente este acceso no autorizado, finalmente, tampoco implementó un plan de migración de datos donde se demostrara que previo a la migración de los datos la sociedad tomó las medidas necesarias para evitar el cruce de identificadores que por ciudad pudiesen quedar repetidos.

Con dicha actuación, el Responsable no solo afectó el derecho de habeas data de los ocho titulares al divulgar su información personal mediante correo electrónico a terceros no autorizados, sino también su derecho a la intimidad. Todos estos Titulares resultaros siendo víctimas de la divulgación de su información personal, pues sus datos se encontraban al alcance de terceros que por un "*error tecnológico*" se cruzaron los (Id) y les permitió el acceso a la información personal a través de un correo de pedido.

Por consiguiente, se encuentra demostrado el incumplimiento por parte de la sociedad **INVERSIONES CMR S.A.S.** del deber establecido en el literal d) del artículo 17 de la Ley 1581 de 2012 por lo que se impondrá la correspondiente sanción.

9.2.3 Respecto del deber de tramitar las peticiones y reclamos presentadas por los titulares

El artículo 15 de Ley 1581 de 2012, establece el término máximo con el que cuentan los Responsables y Encargados del tratamiento para atender los reclamos que ante éstos se presentan y la forma cómo deben hacerlo.

Tal precepto señala que los titulares o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión pueden presentar un reclamo ante el Responsable y/o Encargado del tratamiento, quienes contarán con el término de quince (15) días hábiles para atenderlo, contados a partir de la fecha de recibo del mismo y plazo que podrá prorrogarlo por el término de ocho (8) días hábiles más, previa comunicación al reclamante.

Adicionalmente y sobre el particular, vale la pena hacer referencia al pronunciamiento realizado por la Corte Constitucional en la sentencia C-748 de 2011, cuando al realizar el estudio de constitucionalidad de la Ley 1581 de 2012, se manifestó acerca de las consultas y reclamos que los titulares de la información pueden realizar frente a los Responsables y Encargados del tratamiento, señalando lo siguiente:

> *"Este artículo regula un procedimiento similar al que contempla el artículo 16, II, numerales 1,2 y 3 de la Ley 1266 de 2008, hallado exequible por la Corte en la sentencia C-1011 de 2008.*
>
> *Sobre este mecanismo de reclamos que se consagra ante los responsables y encargados del dato, se puede advertir que los términos que se dieron para que el obligado conteste los requerimientos hechos son los mismos que se consagran para el derecho de petición en el Código Contencioso Administrativo, razón por la que se pueden transpolar los comentarios que se dejaron consignados sobre el carácter instrumental del derecho de petición, en aras de permitir al titular del dato ejercer las facultades que se derivan del habeas data".*

De esta manera, los mecanismos de consultas y reclamos frente a los Responsables y Encargados del Tratamiento, constituye un desarrollo del artículo 23 de la Constitución Política, es decir, la reglamentación del derecho de petición frente a particulares que va específicamente orientado a la salvaguarda del derecho de *habeas data*.

Al respecto, se debe traer a colación el siguiente aparte de la Sentencia C-748 de 2011, que reza:

> *"En consecuencia, el precepto revisado resulta ajustado a la Constitución. No obstante, la Sala debe advertir que la jurisprudencia constitucional ha perfilado unas características que debe tener la respuesta para que se entienda satisfecho el derecho de petición. En ese orden, tanto los responsables como los encargados del tratamiento están obligados a observar esos parámetros que en términos generales se pueden resumir de la siguiente manera: **(i)** la respuesta debe ser de fondo, es decir, no puede evadirse el objeto de la petición, **(ii)** que de forma completa y clara se respondan a los interrogantes planteados por el solicitante, **(iii)** oportuna, asunto que obliga a respetar los términos fijados en la norma acusada".*

Por tanto, es deber de los Responsables y Encargados del Tratamiento garantizar el ejercicio del derecho de *habeas data*, así como garantizar el pleno y efectivo derecho de petición, consulta o reclamación, es decir, atender cada una de las solicitudes de los titulares, sin dilaciones ni atrasos y especialmente, de manera completa y de fondo.

En el caso en concreto, se evidenció que en el desarrollo de la visita de inspección la sociedad **INVERSIONES CMR S.A.S** si bien da respuesta casi inmediatamente a la recepción de las peticiones o reclamos presentados por los titulares, en las mismas se limitan a indicar que la petición fue escalada al área encargada, así mismo, se encuentra lo siguiente respecto de las quejas seleccionadas:

Titular	Número de queja	Hallazgo[13]
[redacted]	[redacted]	No se otorgó respuesta que responda de fondo y de forma completa la petición del titular.
[redacted]	[redacted]	No se otorgó respuesta que responda de fondo y de forma completa la petición del titular.
[redacted]	[redacted]	No se otorgó respuesta que responda de fondo y de forma completa la petición del titular, así como no le informaron las razones técnicas ni administrativas por las cuales le llegaban confirmaciones de pedidos que no había realizado.
[redacted]	[redacted]	No le informaron las razones técnicas ni administrativas por las cuales le llegaban confirmaciones de pedidos que no había realizado.
[redacted]	[redacted]	No le informaron las razones técnicas ni administrativas por las cuales le llegaban confirmaciones de pedidos que no había realizado.
[redacted]	[redacted]	No le informaron las razones técnicas ni administrativas por las cuales le llegaban confirmaciones de pedidos que no había realizado.

Al respecto, la sociedad investigada indicó que *"(...) el hecho de que INVERSIONES CMR cumpla sí o no con los deberes que ostenta en calidad de Responsable de tratamiento de datos personales, es un supuesto que debe establecerse a partir de un análisis completo y detallado del trámite a través del cual esta Empresa recibe, gestiona y resuelve todo tipo de PQRs que le son enviadas por los titulares de la información."* Y que *"(...) la Empresa recibe un gran número (miles) de PQRs relacionadas con diversos temas, razón por la cual un análisis a partir de únicamente ocho (8) solicitudes resulta extremadamente incompleto. La SIC, en su análisis, está omitiendo un gran número de PQRs que fueron recibidas, gestionadas y resueltas de acuerdo con los parámetros establecidos en la norma." (Cuaderno 2 fl.235).*

Es importante aclarar que la Ley 1581 de 2012 en el artículo 19, le confiere la facultad a la Superintendencia de Industria y Comercio para ejercer la función de vigilancia para garantizar que

---

[13] Quejas obrantes en carpeta reservada CD fl.1 y en Cuaderno 1 fls. 51 al 54.

en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la mencionada ley.

Al respecto, resulta relevante establecer que al momento de realizar la visita de inspección del 27 y 28 de octubre de 2015, tal como consta en el acta suscrita el 28 de octubre de 2015 (Carpeta 1 fls.34 al 43) se realizó una búsqueda en la aplicación "Zendesk" en la cual se consolidan todas las PQR's de las peticiones que se han realizado respecto al tratamiento de datos personales, dicha búsqueda arrojó un total de ocho (8) peticiones en las que solicitaban la eliminación o el no envío de correos promocionales, de manera que sobre tal universo de ocho (8) quejas es que se realiza la verificación del cumplimiento del deber establecido en el literal j) del artículo 17 de la Ley 1581 de 2012.

Ahora bien, sobre las peticiones interpuestas en ejercicio del derecho de habeas data, la sociedad investigada indicó que la sociedad tiene dos (2) tipos de bases de datos diferentes: **i)** la base de datos de la aplicación, la cual contiene los datos proporcionados por las personas registradas en domicilios.com vía web o a través de la aplicación móvil; y **ii)** la base de datos de marketing, la cual contiene datos personales de las personas que reciben *news letter*, es decir información relacionada con prospección comercial de la empresa. Y que *"(...) lo único que cambia respecto de la supresión de un usuario de cualquiera de las dos bases de datos, son las personas encargadas de esta supresión, el trámite para llevar a cabo la petición del usuario, y la manera en que el sistema de cada una de las bases de datos procede con la supresión."* (Cuaderno 2 reverso fl.235).

Respecto de la base de datos de la aplicación señaló que *"[a]l eliminar o suprimir datos personales al interior de la base de datos de la aplicación, estos son suprimidos al mismo tiempo que la cuenta del Usuario se elimina de inmediato. Sin embargo, debe tenerse en cuenta que estos datos son eliminados por completo del registro, pero pueden reposar durante un tiempo en los backups que realiza la Empresa."* Y que dicha policita consiste en *"(...) que los datos de un usuario que solicita la supresión permanecen en estos respaldos digitales durante las dos (2) semanas siguientes a la supresión, tiempo después del cual la información es eliminada automáticamente de los servidores. En efecto, esta política ha sido diseñada e implementada con el fin de proteger los datos de la empresa, y asegurar que los mismos puedan ser recuperados en caso de que se presente un fallo de infraestructura."* (Cuaderno 2 reverso fl.235).

Respecto a la base de datos de marketing indicó que "*(...) la supresión al interior de esta base de datos puede darse bien sea i) por solicitud desde el Departamento de Marketing, o ii) por eliminación directa del usuario desde el news letter que recibe en su correo. (...) En este sentido, tal y como puede evidenciarse en la Prueba 5.4, aquella información que persiste al interior de esta base de datos se debe a que el usuario ha continuado usando la plataforma, con posterioridad a tramitar la solicitud de supresión.",* y que "*En el caso presente, por ejemplo, los usuarios que formularon las quejas* [redacted] *; son usuarios que no aparecen en el archivo de usuarios eliminados de la base de datos de marketing, porque estos usuarios hicieron nuevamente uso de la plataforma.*" (Cuaderno 2 fl.236).

Analizando lo manifestado por la investigada, encontramos que aunque la sociedad indica que los titulares de las quejas Nos. [redacted] no se encuentran en el archivo de usuarios eliminados de la base de datos de marketing porque los usuarios hicieron nuevamente uso de la plataforma, no aporta prueba alguna que acredite que efectivamente los titulares utilizaron la aplicación de manera posterior a la petición de supresión.

De otro lado, esta Dirección evidencia que la sociedad investigada no se pronunció respecto a los demás aspectos objeto de investigación respecto a la atención de PQRs, es decir, no se pronunció ni aportó prueba alguna respecto a que: i) no contestaron de fondo y de forma completa las peticiones de los titulares [redacted] queja No. [redacted] y [redacted]; ii) así como no informaron a los ciudadanos [redacted] queja y [redacted] las razones técnicas ni administrativas por las cuales les llegaban confirmaciones de pedido que ellos no habían tenido, puesto que sólo se limitaron a contestarles que la queja había sido escalada al área correspondiente y que tomarían las medidas necesarias.

Por lo anterior, esta Dirección encuentra probado que la sociedad **INVERSIONES CMR S.A.S,** respecto de las quejas mencionadas anteriormente no cumplió con el deber establecido en el literal j) del artículo 17 de la Ley 1581 de 2012, puesto que no demostró haber tramitado las consultas y reclamos presentados por los titulares [redacted] en ejercicio de su derecho de *habeas data* en los términos señalados en la Ley, es decir, atendiendo cada una de las preguntas y solicitudes de los titulares, sin dilaciones ni atrasos, de manera completa y de fondo y dentro del término legal establecido. Por lo que se impondrá la correspondiente sanción.

9.2.4 Respecto del deber de informar a la Superintendencia de Industria y Comercio violaciones a los códigos de seguridad y la existencia de riesgos en la administración de la información personal

De conformidad con la fundamentación fáctica de la investigación de la referencia, el último deber involucrado en el caso *sub-examine* es establecido en el literal n) del artículo 17 de la Ley 1581 de 2012, el cual exige que el Responsable del Tratamiento de los datos personales, al tener conocimiento de posibles riesgos en la administración de la información de los Titulares, informe dichos eventos a la Autoridad de Protección de Datos Personales en Colombia, actualmente la Superintendencia de Industria y Comercio.

En esa medida, se encuentra responsable administrativamente de la trasgresión de este deber a aquellos Responsables del Tratamiento que, al haberse enterado de dicha violación y que la misma haya ocasionado riesgos en el Tratamiento de los datos, no informe a esta Superintendencia de la ocurrencia del incidente de seguridad.

En la visita de inspección se evidenció que, pese a la falla en el proceso de traslado de datos personales, y aun cuando dicho procedimiento puso en riesgo la administración de la información de los titulares cuyos datos fueron objeto de migración, la sociedad investigada no informó a la Superintendencia de Industria y Comercio la ocurrencia de tal situación, pese a estar obligado a ello, en razón a que se configuró un incidente de seguridad.

Al respecto, la sociedad investigada indicó que es necesario informar a la autoridad cuando se presenten violaciones a los códigos de seguridad y cuando también existan riesgos en la administración de la información.

- Respecto a la violación a los códigos de seguridad: indicó que *"(...) la violación a los códigos de seguridad significa que un tercero haya podido acceder a un sistema de información y haya atentado en contra de su seguridad, la cual incluye: disponibilidad, integridad, autenticidad, confidencialidad de los datos. Es por esto que los responsables y encargados del manejo y tratamiento de bases de datos deben contar con herramientas que les permitan afrontar dichos ataques"* y que *"[s]in perjuicio de la implementación de las acciones de mitigación, será necesario que respecto de ataques Dos (Ataques de Denegación de Servicios), los cuales son eventos que atentan contra la seguridad de la información de INVERSIONES CMR, toda vez que altera la disponibilidad de un sistema de información (...) Ejemplo de lo anterior es el informe con radicado No. 16 180684, donde se reportó el incidente menor ocurrido los días 17 y 18 de junio de 2015 (...)".*(Cuaderno 2 fls.237 y 238).

- Respecto a los riesgos en la administración de la información: señaló que *"[d]e conformidad con lo expuesto en las Consideraciones al Cargo Dos, se concluyó que el porcentaje de erro que existió durante el lapso de tiempo especificado por l(sic) SIC fue del 0.8% de una muestra de 450.000, el cual no logra constituir siquiera el 1% y que por lo tanto este porcentaje no se encontraba dentro del nivel óptimo de administración de la información, en tanto sus consecuencias no representan un mayor valor al invertido en administración, esfuerzos y herramientas para la protección de la información y datos personales* (...)".

Sumado a esto, la sociedad investigada asegura que *"(...) es evidente que INVERSIONES CMR nunca expuso a un riesgo en la administración de la información de los cuatrocientos cincuenta mil titulares sobre los cuales posee datos y tampoco fue objeto de una violación a los códigos de seguridad por lo que no debió informar a la SIC, de la manera que lo indica el numeral n) del artículo 17° de la Ley 1581 de 2012, por lo que el cargo no procede."* (Cuaderno 2 fl.238).

Al respecto, esta Dirección encuentra que la sociedad investigada reportó ante esta dirección un ataque relacionado con la denegación del servicio "*DoS*" visible en Cuaderno 2 folio 366 al 380 el cual una vez estudiado, se procedió a archivar por no encontrar afectación a ningún dato de los titulares. La sociedad investigada trae este archivo al caso objeto de investigación con el fin de que sea tenido en cuenta en la valoración del caso, sin embargo, revisado el caso aportado por la investigada de radicado No. 16-180684 encontramos que en el mismo i) no se presentó una fuga de información o acceso no autorizado a los datos personales y ii) se bloquearon las direcciones IP desde donde se realizaron los ataques de denegación de servicio "*DoS*".

Así pues, encontramos que en el caso de radicado 16-180684 no se encontró afectación a ningún titular, es decir que no se tuvo acceso no autorizado a los datos de los titulares, no obstante, en el caso bajo estudio, se encuentra demostrado y es aceptado por la sociedad[14] que terceros no autorizados tuvieron acceso, aunque no voluntario o premeditado, a los datos personales de los titulares a través de una difusión no autorizada de correos de confirmación de domicilio, dada por error humano interno al momento de realizar la migración de los datos.

Mediante la Circular Externa No. 002 del 3 de noviembre de 2015, la Superintendencia de Industria y Comercio amplió el espectro de interpretación de los incidentes de seguridad, al establecer en el Capítulo 2 que todos los Responsables y Encargados de Tratamiento deberán reportar en el Registro Nacional de Bases de Datos, "*la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado*" a sus bases de datos dentro de los quince (15) días hábiles posteriores al momento en que sean detectados y se pongan en conocimiento del área encargada de atenderlas.

Como se aprecia, la norma es clara en definir que "*incidente de seguridad*" se refiere a la "*violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado*", definición que resulta bastante más amplia que la contenida en el literal n) de la Ley, pues este sólo habla de "*violaciones a los códigos de seguridad*" sin referirse a la "*perdida, robo y/o acceso no autorizado*". Bajo dicho razonamiento es que **INVERSIONES CMR S.A.S**. insiste en que en el presente caso "nunca existió un peligro inminente al que se vieran expuestos los titulares de los datos", toda vez que, a juicio de la investigada, "*respecto de los ataques DoS (Ataques de Denegación de Servicios), los cuales son eventos que atentan contra la seguridad de la información de INVERSIONES CMR, toda vez que altera la disponibilidad de un sistema de información (...)*" (reverso carpeta 2 fl.440), es decir, que para la investigada el hecho de que un tercero no autorizado reciba correos con información personal de los titulares no es un incidente de seguridad pues no altera la disponibilidad de un sistema de información, evento en el cual se genera un error en la adecuación típica de la falta administrativa.

Para resolver la presente cuestión, se considera necesario realizar dos análisis distintos: (i) la disposición contenida en el artículo 2.2.2.25.3.7 del Decreto Único Reglamentario 1074 de 2015 para que la Superintendencia de Industria y Comercio "*imparta las instrucciones relacionadas con las medidas de seguridad en el Tratamiento de datos personales*" y su integración con la Circular Externa No. 002 del 3 de noviembre de 2015, y (ii) la interpretación del deber contenido en el literal n) del artículo 17 de la Ley 1581 de 2012, en específico, el concepto de "*violaciones a los códigos de seguridad*".

(i) Del artículo 2.2.2.25.3.7 del Decreto Único Reglamentar 1074 de 2015 y su integración con la Circular Externa No. 002 del 3 de noviembre de 2015

El artículo 2.2.2.25.3.7 del Decreto Único Reglamentario 1074 de 2015 indica lo siguiente:

> "*Medidas de seguridad. La Superintendencia de Industria y Comercio impartirá las instrucciones relacionadas con las medidas de seguridad en el Tratamiento de datos personales*".

La Circular Externa No. 002 describe, dentro de su fundamento legal, que para el adecuado ejercicio de las funciones de vigilancia en materia de protección de datos personales atribuidas por

---

[14] En contestación a peticiones y quejas de los titulares ante el envío de correos de confirmación de pedidos con datos personales a terceros, la sociedad reconoce el hecho indicando lo siguiente "*Lamentamos lo ocurrido con su solicitud, verificamos en el sistema y por motivos de actualización de la página ocurrió este error (...)*" (visible Carpeta 1 fl.14).

el legislador, la SIC diseñó un sistema basado en riesgos: el Sistema Integral de Supervisión Inteligente – SISI, el cual proveerá de información relacionada con las bases de datos objeto de tratamiento. Por su parte, el artículo 25 de la Ley 1581 de 2012, creó el Registro Nacional de Bases de Datos –RNBD-, definido legalmente como "*el directorio público de las bases de datos sujetas a Tratamiento que operan en el país*". Por ello, la referida circular continúa señalando en su fundamento legal que:

> *"El Capítulo 26 del Decreto Único 1074 de 2015 reglamentó el artículo 25 de la Ley 1581 de 2012 y estableció la información mínima que debe contener el Registro, así como los términos y condiciones de inscripción. En particular, en el artículo 2.2.2.26.2.1, el citado decreto señaló que "(l)a Superintendencia de Industria y Comercio, como autoridad de protección de datos personales, podrá establecer dentro del Registro Nacional de Bases de Datos información adicional a la mínima prevista en este artículo, acorde con las facultades que le atribuyó la Ley 1581 de 2012 en el literal h) del artículo 21". Así mismo, en el artículo 2.2.2.26.3.2 dispuso que "(l)a Superintendencia de Industria y Comercio establecerá el procedimiento de inscripción en el Registro Nacional de Bases de Datos que deberán cumplir los Responsables del Tratamiento, previa validación de su identidad, de acuerdo con lo que para el efecto establezca esa entidad".*
>
> *Por lo expuesto, se hace necesario establecer la información adicional que contendrá el Registro Nacional de Bases de Datos – RNBD - y el procedimiento de inscripción (i) para que los Responsables del Tratamiento de datos personales, personas naturales, entidades de naturaleza pública distintas de las sociedades de economía mixta y personas jurídicas de naturaleza privada que no están inscritas en las cámaras de comercio, cumplan con este deber legal y (ii) la Superintendencia de Industria y Comercio ejerza de manera eficiente sus funciones de vigilancia en materia de protección de datos personales."*

Como se ve, la Circular Externa No. 002 del 3 de noviembre de 2015 no prevé, dentro de su objeto, desarrollar el contenido del artículo 2.2.2.25.3.7 del Decreto 1074 de 2015, referido a las medidas de seguridad en el tratamiento de datos personales; sino que busca establecer la información mínima contenida en el registro, complementado así lo previsto en el Capítulo 26 del mismo decreto único[15], el cual se ocupa precisamente, del RNBD.

Entonces, es claro que se trata de una norma complementaria para la adecuada administración del RNBD, cuya responsabilidad se encuentra en cabeza de esta Superintendencia. Sin embargo, es claro que todas las leyes, decretos y resoluciones que se expidan desarrollando las facultades de esta Superintendencia como Autoridad de Protección de Datos, conforman el sistema Colombiano de protección de datos personales, en el cual cada componente normativo debe interpretarse armónicamente, por lo que resulta válido aplicar en un caso específico la conceptualización de incidente de seguridad contenida en el capítulo 2 de la Circular.

En este orden de ideas, si bien no es posible aplicar en el caso en concreto la disposición contenida en la circular debido al principio de irretroactividad, pues los hechos materia de investigación se configuraron con anterioridad al 3 de noviembre de 2015, también lo es que la definición de "*incidente de seguridad*" no depende exclusivamente de la circular, pues la misma Ley 1581 de 2012, dispuso en su articulado medidas relacionadas con el deber de seguridad que deben cumplir los Responsables y existen documentos que permiten definir dicho concepto, situación que se analizará a continuación.

(ii) Disposiciones relacionadas con la seguridad de la información y la interpretación del deber contenido en el literal n) del artículo 17 de la Ley 1581 de 2012, en específico, el concepto de "violaciones a los códigos de seguridad"

La sociedad **INVERSIONES CMR S.A.S.** no puede justificar su incumplimiento al deber de informar a la Autoridad de Protección de Datos de la materialización de una violación a los códigos de seguridad bajo los argumentos de que para que se presente una violación a los códigos de seguridad en la medida en que para que opere se debe *"alterar la disponibilidad de un sistema de información*". Ahora, lo que corresponde a este Despacho es, precisamente determinar el alcance de la expresión "*violaciones a los códigos de seguridad*".

---

[15] Capítulo 26 del Decreto Único Reglamentario 1074 de 2015; Registro Nacional de Bases de Datos.

Pues bien, el artículo 17 de la Ley 1581 de 2012, consagra los deberes de los Responsables del tratamiento, e indica, en su literal n), que estos deberán *"(i)nformar a la autoridad de protección de datos cuando se presente violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares"*.

Coincide este Despacho con la investigada, cuando esta afirma que para que se configure el supuesto contenido en la norma, deben presentarse dos situaciones: por un lado i) la existencia de violaciones a los códigos de seguridad y ii) que existan riesgos en la administración de la información de los titulares. En su sentido natural y obvio, es claro que los riesgos deben recaer sobre la información personal y que estos son producto, esencialmente, de la violación a un determinado código de seguridad.

Bajo esta hipótesis, no se adecuaría la descripción contenida en la norma cuando se presente una violación de un código de seguridad de una base de datos que no conteniente información personal. Tampoco sería objeto de dicho deber cuando, a pesar de que se presentó la referida violación, no existe un riesgo en la administración de la información de los titulares, bien sea porque se cuenta con otras medidas de control para mitigar el mismo, o porque la violación no comprometió información personal, entre otras posibilidades.

<u>El principio y deber de seguridad de la información</u>

El legislador en el artículo 3 de la Ley 1581 de 2012, desarrolló unos determinados principios en materia de protección de datos personales, los cuales, a su vez, permean la interpretación de todos los artículos contenidos en la Ley 1581 de 2012 y sus decretos reglamentarios, por lo que cualquier exégesis de las normas previstas en dicho estatuto debe realizarse de conformidad con los principios, ya que estos delimitan las fronteras de aplicación de las normas por cuya observancia debe velar esta entidad. Además, resulta claro que los principios, como criterio interpretativo que son, se encuentran plenamente armonizados con los derechos de los titulares del dato y los deberes de los sujetos obligados en la Ley.

En efecto, para la Corte Constitucional la cuestión es de la siguiente manera:

> *"Estos principios [los contenidos en la ley], buscan impedir el uso abusivo y arbitrario de la facultad informática. Así mismo, deben ser interpretados en concordancia con el segundo inciso del artículo 15 de la Carta, que establece que "(e)n la recolección, tratamiento y circulación de los datos se respetarán la libertad y demás garantías consagradas en la Constitución".*
>
> *Es decir, el artículo 4 de la Ley Estatutaria define el contexto axiológico dentro del cual debe moverse, el proceso informático. Según este marco general, existen unos parámetros generales que deben ser respetados para poder afirmar que el proceso de acopio, uso y difusión de datos personales sea constitucionalmente legítimo."*

Tal circunstancia es clara si se observa el tenor del literal del artículo 4, cuando señala que *"[e]n el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios (...)"*, de lo que resulta claro que este Despacho no pretende realizar ningún tipo de extensión indebida de la ley en su aplicación a áreas de interpretación vedadas por el legislador, pues se busca que las normas contenidas en el régimen de protección de datos personales se interpreten como un todo, siempre teniendo presente el espíritu teleológico de la norma.

De esta forma, dentro de estos mandatos interpretativos, el legislador estatutario incluyó, entre otros, el principio de seguridad ya mencionado en la presente resolución, pero que debido a su importancia para el caso es necesario analizar desde otra perspectiva.

En virtud del mencionado principio, *"[l]a información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento"*, lo cual implica que los sujetos obligados de la ley deberán disponer de las medidas necesarias para asegurar la información objeto de procesamiento.

El principio de seguridad a su vez, se encuentra desarrollado como deber legal de los Responsables del tratamiento, toda vez que el literal d) del artículo 17 de la Ley 1581 de 2012 señala que estos deberán "*[c]onservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento*".

Resulta palmaria la relación complementaria del citado deber con aquel referido a la obligación de informar a la autoridad cuando se producen violaciones a los códigos de seguridad, pues mientras el literal d) del artículo 17 dispone la necesidad de implementar las medidas de seguridad adecuadas y suficientes para preservar los datos personales de los titulares, el literal n) señala que cuando dichas medidas falles y se ponga en riesgo la administración de la información, tal situación debe ponerse en conocimiento de la SIC.

Esta relación intrínseca entre el principio de seguridad y los deberes previstos en los literales d) y n) del artículo 17, permite establecer un punto de conexión que brinda claridad sobre una serie de presupuestos que se deban presentar para la configuración típica de la conducta concreta bajo estudio, esto es, el deber de informar a la autoridad de la violación a los códigos de seguridad:

- El principio y el deber de seguridad disponen que se deben implementar las medidas necesarias[16] para evitar la "adulteración, perdida, consulta, uso o acceso no autorizado o fraudulento"[17];

- Que una vez implementados estos mecanismos adecuados para conservar y proteger la información personal en cumplimiento del principio y deber de seguridad, se produzca un evento que viole, incumpla, infrinja o rompa los códigos de seguridad adoptados para preservar la base de datos personales;

- Que el referido evento que afecta los mecanismos de control y seguridad dispuestos por el Responsable ponga en riesgo la administración de la información personal.

Así las cosas, es claro que debe existir una relación entre la medida de seguridad adoptada –o inclusive la falta de ella- el incidente que afecta la base de datos y el riesgo que tal incidente genera en la gestión de la información personal de los titulares.

De las medidas preventivas y el concepto de "violaciones a los códigos de seguridad"

Una vez revisada la descripción literal del principio y el deber de seguridad, es notorio que estos no establecen específicamente cuales son las medidas conducentes para brindar seguridad a los registros para evitar la "*adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento (de la información)*", no obstante, sí señala que deben implementarse las medidas necesarias. Es más, el mismo artículo 2.2.2.25.6.1 del Decreto 1074 de 2015, el cual introdujo en la normatividad nacional el concepto de *Accountability* o responsabilidad demostrada, hace énfasis en dicha situación, cuando dispone que *"[l]os 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 los siguiente*** *(...)"* (Negrilla fuera de texto).

De lo anterior, queda claro que corresponde, en principio, a los Responsable -y por extensión normativa a los Encargados-, demostrar al ente de control que dispusieron de las medidas de seguridad apropiadas para la conversación de la información que es objeto de los tratamientos por ellos definidos, por lo que son estos quienes definirán tales controles, de acuerdo a los cuatro supuestos fundamentales contenidos en el artículo 2.2.2.25.6.1 del Decreto 1074 de 2015, el cual indica 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, media o gran empresa, de acuerdo con la norma vigente.*

---

[16] Las que considere el Responsable.

[17] Esta descripción se repite en el principio de seguridad del literal g) del artículo 4 de la Ley 1581 de 2012 y en el deber de seguridad del literal d) del artículo 17 de la misma norma.

2. La naturaleza de los datos personales objeto del tratamiento.

3. El tipo de Tratamiento.

4. Los riesgos potenciales que el referido tratamiento podría causar sobre los derechos de los titulares".

Para despejar el panorama sobre este tema, el 28 de mayo de 2015, la SIC realizó el lanzamiento de las "*Guías para la Implementación del Principio de Responsabilidad Demostrada (Accountability)*", documento que busca que las organizaciones asumen el compromiso de incrementar sus estándares de protección en el tratamiento de la información personal, a través de algunas pautas que les ayuden a hacer más eficientes sus procedimientos y contribuyan en el propósito de construir un Programa Integral de Gestión de Datos Personales.

En las mencionadas guías se describe un "PROTOCOLO DE RESPUESTA EN EL MANEJO DE VIOLACIONES E INCIDENTES"[18], en el que se hace referencia, precisamente, al concepto de incidente de seguridad en los siguientes términos:

> "***Los incidentes se refieren a cualquier evento en los sistemas de información*** *o bases de datos manuales o sistematizadas, que atente contra la seguridad de los datos personales en ellos almacenados. La Ley 1581 de 2012 no hace distinción alguna respecto de los incidentes que deben ser reportados a la Superintendencia, por lo que,* ***independientemente de su impacto, deben reportarse a esta entidad todos los incidentes ocurridos****. Como mínimo, debe informarse el tipo de incidente, la fecha en que ocurrió y la fecha en la que se tuvo conocimiento del mismo, la causal, el tipo de datos personales comprometidos y la cantidad de titulares afectados."* (Negrilla fuera de texto).

Como se ve, el concepto transcrito es claro en determinar **que cualquier suceso en los sistemas de información que atente contra la seguridad de los datos personales almacenados en una base de datos se constituye en un incidente**, por lo que es claro que, contrario a lo que afirma la investigada, el caso bajo estudio donde terceros accedieron a la información personal de los titulares sin autorización atenta la seguridad de los datos, así pues, cualquier compromiso para la seguridad de los registros es suficiente para adquirir la consideración de incidente.

Si bien, las referidas guías no pueden constituirse en una norma vinculante y de obligatorio cumplimiento pues escapan a la tradicional concepción de las normas jurídicas propiamente dichas, sí constituyen un criterio de orientación -por ello son una guía- que puede ser tenido en cuenta por aquellos que realizan actividades que involucran el manejo de información personal. Es esta, quizá, una manifestación de la tendencia del derecho público a acercarse al concepto de *soft law*, normas *cuasi legales* que no son coercitivas a pesar de que pueden estar construidas como reglas, pero que, en todo caso, buscan influir en la conducta de sus destinatarios.

Así pues, el concepto de incidente de seguridad contenido en las "*Guías para la Implementación del Principio de Responsabilidad Demostrada (Accountability)*", es un criterio que pudo -y debió- ser tenido en cuenta por la sociedad INVERSIONES CMR S.A.S. al momento de evaluar si se estaba en presencia de un evento en el cual debía informar a la autoridad de control del riesgo en la administración de los datos personales que trata. Igual, es claro que las referidas guías se publicaron el 28 de mayo de 2015, esto es, con anterioridad a la fecha en que se evidencian los reclamos presentados informando sobre el envío erróneo de correos con información personal.

El análisis semántico de la expresión "violar" conlleva a considerar que dicha palabra goza de distintas acepciones en el Diccionario de la Lengua Española; entre ellas, se destaca "[i]nfringir o quebrantar una ley, un tratado, un precepto, una promesa, etc."[19], de lo cual se predica que la

---

[18] En su capítulo 2.6, el referido documento señala que *"[l]as violaciones a los códigos de seguridad de las organizaciones generan un altísimo riesgo para los titulares de la información y son causantes en muchos casos de impactos muy significativos a la reputación corporativa. Por lo anterior, un Programa Integral de Gestión de Datos Personales debe involucrar un componente de gestión de riesgos, internos y externos, que le permita identificar sus vulnerabilidades a tiempo y enfocar sus recursos a la adopción de medidas de mitigación de riesgo que minimicen dicho impacto tanto para la organización como para los titulares de la información*".

[19] Real Academia Española, Diccionario de la lengua española. Del texto: "*violar*" (online) Disponible en http://dle.rae.es/?id=braKubl (Recuperado el 11 de mayo de 2016).

palabra puede hacer referencia a una situación contraría a una regla o un principio, sin importar que esta sea jurídica o no.

Tal definición lleva esta Dirección a considerar que las "*violaciones a los códigos de seguridad*" pueden ser aquellos eventos que infrinjan o rompan una medida de seguridad dispuesta. Inclusive, a partir de un análisis interpretativo del citado precepto -y siempre teniendo en cuenta el espíritu teleológico de la norma-, por lo que no es posible concluir que el legislador únicamente pretendió que se reportaran a la SIC aquellas situaciones en las que terceros, dolosamente o intencionalmente, vulneraran una medida de seguridad informática o simplemente aprovecharan la ausencia de un control para poner el riesgo la información personal de los titulares, pues lo que preocupa a la norma no es la intencionalidad del sujeto sino el riesgo que genera dicha situación en la "*administración de la información de los Titulares*".

Entonces, es claro que la sociedad **INVERSIONES CMR S.A.S** incurre en error cuando afirma que la sociedad "no cumplió ninguno de los dos requisitos necesarios para desencadenar el deber indicado en el numeral n). Puesto que existe un deber de informar a una autoridad administrativa una situación objetiva -lo cual no es lo mismo que considerar que existe una responsabilidad objetiva-, que no es otra que la violación de un código de seguridad que ponga en riesgo la administración de datos personales de los titulares, sin llegar a considerar que dicha violación sea producto de una intromisión arbitraria a un sistema de información o afirmar erróneamente como lo hace la investigada, que únicamente sea respecto de ataques DoS que alteren la disponibilidad de un sistema de información.

En virtud de lo expuesto, este Despacho concluye que en el presente caso la sociedad **INVERSIONES CMR S.A.S.** debió informar a la Sic que se presentó un evento que puso en riesgo los datos personales de los titulares.

Lo anterior, con base en que se encuentra demostrado que se presentaron violaciones a los códigos de seguridad de la sociedad investigada permitiendo el envío de correos electrónicos con información personal de sus clientes a terceros no autorizados y existieron riesgos en la administración de la información puesto que la sociedad tiene el deber de velar por la disponibilidad, integridad y confidencialidad de la información de la cual actúa como Responsable del tratamiento, y en el caso en estudio, se afectó la confidencialidad de la información al presentarse un acceso involuntario no autorizado por parte de terceros, así que independientemente de la cantidad de titulares afectados, se presentó un incidente de seguridad al presentarse una falla en el proceso tecnológico de migración de datos que generó que lo identificadores (Id) de los titulares que realizaban pedidos se cruzaran con los identificadores (Id) de otros titulares por el proceso de unificación de las bases de datos en una plataforma. Por lo que se impondrá la correspondiente sanción.

DÉCIMO: Imposición y graduación de la sanción

Respecto a las sanciones que se imponen por la infracción al Régimen de Protección de Datos, debe precisarse que conforme al principio de proporcionalidad que orienta el derecho administrativo sancionador, la autoridad administrativa debe ejercer su potestad sancionatoria en forma razonable y proporcionada, de modo que logre el equilibrio entre la sanción y la finalidad de la norma que establezca, así como la proporcionalidad entre el hecho constitutivo de la infracción y la sanción aplicada. Sobre la aplicación de este principio, la Corte Constitucional ha señalado:

> *"En cuanto al principio de proporcionalidad en materia sancionatoria administrativa, éste exige que tanto la falta descrita como la sanción correspondiente a las mismas que resulten adecuadas a los fines de la norma, esto es, a la realización de los principios que gobiernan la función pública. Respecto de la sanción administrativa, la proporcionalidad implica también que ella no resulte excesiva en rigidez frente a la gravedad de la conducta, ni tampoco carente de importancia frente a esa misma gravedad"*[20]

De esta forma, para la correcta adecuación de los hechos y la sanción aplicable, el operador jurídico en materia de protección de datos personales, debe en primera medida analizar la dimensión del daño o peligro a los intereses jurídicos tutelados, así como el posible beneficio económico, para

[20] Corte Constitucional, Sala Plena, Sentencia C-125 del 18 de febrero de 2003, Exp. Rad. D-4059, Magistrado Ponente Dr. Marco Gerardo Monroy Cabra.

luego analizar otras circunstancias concurrentes de graduación, tales como la capacidad económica del investigado, la reiteración de la infracción, colaboración del investigado para esclarecer los hechos investigados[21].

También se tendrán en cuenta para la dosificación de la sanción, el tamaño de la empresa, sus ingresos operacionales, patrimonio y, en general, su información financiera, de tal forma que la sanción resulte disuasoria más no confiscatoria. Finalmente, se tendrán en cuenta la conducta de la investigada durante el trámite de la investigación administrativa.

En el caso sub-examine, en primer término, quedo demostrado que la sociedad investigada incumplió el deber de solicitar y conservar copia de la autorización previa y expresa de los titulares (seleccionados aleatoriamente) para el tratamiento de sus datos, al no aportar copia de las autorizaciones previas y expresar otorgadas por los titulares a la sociedad para el tratamiento de sus datos personales, así como tampoco demostró cumplir con el deber de informar a estos ocho (8) titulares de manera clara y expresa el tratamiento al cual serán sometidos sus datos, la finalidad del mismo, los derechos que les asisten como titulares y los datos de identificación y contacto del Responsable del tratamiento.

Frente a lo mencionado, este Despacho considera que al no haber solicitado y conservado la autorización de los titulares así como informado las finalidades del tratamiento, vulneró el derecho fundamental de habeas data de los titulares al mantener y tratar datos personales sobre los cuales no contaba con el consentimiento de los titulares, así como impidió a los titulares conocer las finalidades específicas para las cuales fueron recolectados sus datos, el tipo de tratamiento que realizan sobre los mismos y los derechos que le asisten y medios para ejercerlos, por lo que se impondrá una multa por la vulneración de los deberes que ostenta en su calidad de Responsable de la información contemplados en el artículo 9 y 12 y los literales b) y c) del artículo 17 de la Ley 1581 de 2012, en concordancia con lo establecido en el artículo 2.2.2.25.2.5 del Decreto 1074 de 2015, equivalente a cuarenta (40) salarios mínimos legales mensuales vigentes.

En segundo término, quedo demostrado que a pesar de las explicaciones presentadas por la sociedad investigada no existe justificación válida para no haber conservado la información personal de los titulares sobre los cuales sus datos personales fueron enviados a terceros mediante correo o mensaje de confirmación de pedido, bajo las medidas de seguridad que demandaban. En este sentido, esta Dirección tiene en cuenta que efectivamente fueron divulgados, sin ningún tipo de control, a través de mensajes de confirmación de pedido, los datos personales tales como nombre completo, dirección de residencia, teléfono de los usuarios sobre los cuales por un error tecnológico se cruzaron los Id permitiendo el envío a terceros.

En consecuencia, no hay lugar a dudas para esta Dirección acerca de la dimensión del daño que efectivamente se materializó en el caso en cuestión al no conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, y aún más después de que la sociedad tuvo conocimiento del envío erróneo de correos con datos personales a terceros no autorizados, la misma no tomó medidas a tiempo para corregir esto con el fin de que no continuara sucediendo y tampoco implementó un plan de migración de datos donde tomará las medidas necesarias para evitar el cruce de identificadores.

Por lo anterior, esta Dirección considera que la sociedad vulneró el derecho de *habeas data* de los titulares al conocer de este acceso no autorizado de información personal, y no haberse adoptado las medidas técnicas, humanas y administrativas de seguridad antes para evitar que pasara y posteriormente con el fin de corregir e impedir que continuara sucediendo, se vulneró el derecho fundamental de habeas data de los titulares, e incluso puso en peligro otros derechos fundamentales como la intimidad, por lo que se impondrá una multa por la vulneración del deber

---

[21] Ley 1266 de 2008 "*Artículo 19. 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 expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.*"

establecido en el literal d) del artículo 17 de la Ley 1581 de 2012, equivalente a noventa (90) salarios mínimos legales mensuales vigentes.

En tercer término, la sociedad vulneró el derecho fundamental de los titulares al no cumplir con el deber establecido en el literal j) del artículo 17 de la Ley 1581 de 2012,en concordancia con los artículos 14 y 15 de la norma en mención, es decir que no demostró haber tramitado las consultas y reclamos presentados por los titulares en ejercicio de su derecho de *habeas data* en los términos señalados en la Ley, es decir, atender cada una de las preguntas y solicitudes de los titulares, sin dilaciones ni atrasos, de manera completa y de fondo y dentro del término legal establecido. Impidiéndole así ejercer a los titulares plena y efectivamente su derecho fundamental de habeas data tendiente a conocer, actualizar y rectificar su información. Por lo que se impondrá una multa equivalente a ochenta (80) salarios mínimos legales mensuales vigentes.

Finalmente, en cuarto término, respecto del deber de informar a esta Superintendencia cuando se presenten violaciones a los códigos de seguridad que generen riesgos en la administración de los datos personales de los titulares, esta Dirección considera que el legislador estatutario incorporó a la norma dicha obligación legal buscando minimizar el riesgo para la información que de tal situación se puede desprender y que se adopten las medidas conducentes para evitar la afectación de derechos fundamentales como la intimidad y el *habeas data*.

Sin embargo, al no informarse a esta entidad de la configuración del incidente de seguridad, la sociedad **INVERSIONES CMR S.A.S.** incumplió su deber legal y una vez conocido el incidente no tomó las medidas apropiadas para solucionar dicha situación por lo que continuó generándose el acceso a terceros no autorizados de los datos personales.

Comoquiera que **INVERSIONES CMR S.A.S.** no observó el cumplimiento del deber para salvaguardar la información que, con ocasión al Tratamiento que realiza de la misma, le fue suministrada por los usuarios de la aplicación, bajo las condiciones necesarias para impedir su acceso no autorizado, esta Superintendencia, al tenor del inciso primero del artículo 23 de la Ley Estatutaria de Protección de Datos Personales, impondrá una multa de ochenta (80) salarios mínimos legales mensuales vigentes, por el incumplimiento del deber establecido en el literal n) del artículo 17 de la Ley 1581 de 2012, puesto que se presentó un acceso no autorizado involuntario de la información personal por parte de terceros.

10.1 *Otros criterios de graduación*

Por último se aclara que los criterios de graduación de la sanción señalados en los literales b), c), d), e) y f) del artículo 24 de la Ley 1581 de 2012 no serán tenidos en cuenta debido a que (i) dentro de la investigación realizada 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 citado no se aplica toda vez que el investigado no reconoció o aceptó la comisión de la infracción.

En mérito de lo expuesto este Despacho,

RESUELVE

ARTÍCULO PRIMERO: Imponer una sanción pecuniaria a la sociedad **INVERSIONES CMR S.A.S** identificada con el Nit. 900.129.597-5, de **DOSCIENTOS TRECE MILLONES NOVECIENTOS TRENTA Y SIETE MIL NOVECIENTOS TREINTA PESOS M/cte. ($213.937.930)**, equivalente a doscientos noventa (290) salarios mínimos legales mensuales vigentes, por los hechos descritos en la parte motiva de esta providencia.

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. En el recibo deberá indicarse el número del expediente y el número de la presente resolución. El pago deberá acreditarse ante la pagaduría de esta Superintendencia,

con el original de la consignación, dentro de los cinco (5) días hábiles siguientes a la ejecutoria de esta resolución.

ARTÍCULO SEGUNDO: Notificar personalmente el contenido de la presente resolución a la a la sociedad **INVERSIONES CMR S.A.S** identificada con el Nit. 900.129.597-5, 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 el de apelación ante el Superintendente Delegado para la Protección de Datos Personales, dentro de los diez (10) días siguientes a la diligencia de notificación.

ARTÍCULO TERCERO: Comuníquese el contenido de la presente resolución al señor [redacted] identificado con la cedula de ciudadanía No. No. [redacted]

NOTIFÍQUESE, COMUNÍQUESE Y CÚMPLASE
Dada en Bogotá D. C.,

El Director de Investigación de Protección de Datos Personales, 30 NOV. 2017

CARLOS ENRIQUE SALAZAR MUÑOZ

Proyectó: AMVJ
Revisó: CESM
Aprobó: CESM

NOTIFICACIÓN:

Investigada:
Entidad: **INVERSIONES CMR S.A.S.**
Identificación: Nit. 900.129.597-5
Representante legal suplente: [redacted]
Identificación: C.C. No. [redacted]
Dirección: Calle 94 No. 16 - 60
Ciudad: Bogotá, D.C.
Correo electrónico: jcalderon@clickdelivery.com

Apoderado especial: [redacted]
Identificación: C.C. No. [redacted]
Dirección: [redacted]
Ciudad: [redacted]

COMUNICACIÓN

Titular de la información:
Señor: [redacted]
Identificación: C.C. No. [redacted]
Apoderado: [redacted]
Identificación: C.C. No. [redacted]
Dirección: [redacted]
Correo electrónico: [redacted]