

REPÚBLICA DE COLOMBIA



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

RESOLUCIÓN NÚMERO 48960 DE 2021

(Agosto 3 de 2021)

Radicación 18-26450

VERSIÓN PÚBLICA

**EL SUPERINTENDENTE DELEGADO PARA LA PROTECCION DE DATOS PERSONALES**

En ejercicio de sus facultades legales, en especial las conferidas por los artículos 19 y 21 de la Ley 1581 de 2012 y el numeral 7 del artículo 16 del Decreto 4886 de 2011 y,

**CONSIDERANDO:**

**PRIMERO:** Que mediante oficio radicado con el número 18-26450-00 de 19 de enero de 2018, la señora [REDACTED], presentó ante esta Superintendencia queja en contra de **CREDIVALORES – CREDISERVICIOS S.A.** (en adelante **CREDIVALORES**), pues consideró vulnerado su derecho de *habeas data*, y de la cual se extrae lo siguiente:

*PRIMERO: El día Veintiséis [sic] (26) de Junio de Dos Mil Dieciséis (2.016) adquirí una tarjeta de crédito "CREDIUNO" en las instalaciones del Centro Comercial Único de la ciudad de Cali, suministrando la dirección de mi residencia, mi correo electrónico y teléfono celular con el fin de que fueran enviados los extractos de la misma, o en su defecto ser contactada para cualquier novedad relacionada con lo mismo.*

*SEGUNDO: El día Diecisiete [sic] (17) de Octubre [sic] de Dos [sic] Mil [sic] Diecisiete [sic] (2.017) [sic] con extrañeza me fue informado que el extracto de la tarjeta había sido enviado al correo [REDACTED], el cual NUNCA suministre a la entidad, toda vez que corresponde a una persona de la cual no tengo contacto hace más de dos años.*

*TERCERO: Igualmente, en días anteriores fue contactado el jefe de mi pareja, para informarle alguna novedad del pago de la tarjeta, del cual, nuevamente manifiesto NUNCA suministre el teléfono celular de él, toda vez que es una persona con la que no tengo relación alguna.*

*CUARTO: En atención a lo anteriormente [sic] manifestado, envíe una petición mediante la página web [www.credivalores.com/Servicio al Cliente/ContáctenosSQL](http://www.credivalores.com/Servicio al Cliente/ContáctenosSQL), solicitando información de los datos y correos que tienen en referencia con mi información.*

*QUINTO: En relación al acápite anterior, el día Veintiséis [sic] (26) de Octubre [sic] recibí mediante correo electrónico respuesta con radicado No. 2693599 donde me manifestaron que los datos habían sido actualizados, pero no dieron respuesta a lo que realmente se había solicitado.*

*SEXTO: Nuevamente el día Dos [sic] (2) de Noviembre del año en curso, solicite [sic] la misma información que ya había solicitado pero que no me dieron respuesta, a la fecha todavía me encuentro esperando dicha información.*

*SEPTIMO: El día 9 de diciembre realizo un derecho de petición solicitando lo siguiente:*

- 1. Solicito cordialmente me sea informado de que fuente adquirieron datos de otras personas para suministrarle mi información relacionada con los servicios que tengo con ustedes.*
- 2. En atención a la petición anterior, solicito que dichos datos sean eliminados y suprimidos teniendo en cuenta que no corresponden a la suscrita.*

*OCTAVO: En ninguna de las respuestas se cumple con la primer solicitud, no obstante el día Dieciséis [sic] (16) de Enero [sic] de Dos [sic] Mil [sic] Dieciocho [sic] (2.018) con extrañeza me fue informado que el extracto de la tarjeta había sido enviado nuevamente al correo [REDACTED], el cual reitero NUNCA suministre a la entidad. Me preocupa mucho que no tengo conocimiento de quién más está recibiendo mi información privada.*

**SEGUNDO:** Que mediante Resolución 53886 de 11 de octubre de 2019, el Director de Investigación de Protección de Datos Personales resolvió iniciar una investigación administrativa y formular cargos, con el fin de establecer si **CREDIVALORES** infringió las normas sobre protección de Datos personales, que se relacionan a continuación:

- (i) El literal a) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal d) del artículo 4 de la misma ley, y con el artículo 2.2.2.25.4.3 del Decreto Único Reglamentario 1074 de 2015.
- (ii) El literal b) de artículo 17, en concordancia con el literal c) del artículo 4 y el artículo 9 de la Ley 1581 de 2012, así como con el inciso primero del artículo 2.2.2.25.2.2 del Decreto Único Reglamentario 1074 de 2015.

- (iii) El literal c) del artículo 17, en concordancia con el literal b) del artículo 4, el literal a) del artículo 12 de la Ley 1581 de 2012, así como con el inciso primero del artículo 2.2.2.25.2.2 del Decreto Único Reglamentario 1074 de 2015.
- (iv) El literal d) del artículo 17, en concordancia con el literal g) del artículo 4 de la Ley 1581 de 2012.
- (v) El literal j) del artículo 17 en concordancia con el artículo 14 y el literal e) del artículo 4 de la Ley 1581 de 2012.
- (vi) El literal j) del artículo 17 en concordancia con el artículo 15 de la Ley 1581 de 2012.
- (vii) El literal o) del artículo 17 de la Ley 1581 de 2012.

**TERCERO:** Que una vez agotada la etapa probatoria y efectuado el análisis y de los diferentes medios probatorios allegados oportunamente a la presente actuación administrativa, el Director de Investigación de Protección de Datos Personales resolvió, mediante la Resolución No. 46328 de 11 de agosto de 2020, lo siguiente:

**"ARTÍCULO PRIMERO: IMPONER** una sanción pecuniaria a la sociedad **CREDIVALORES – CREDISERVICIOS S.A.**, identificada con NIT 805.025.964-3 de **CUATROCIENTOS VEINTIÚN MILLONES TRESCIENTOS TREINTA Y SIETE MIL SEISCIENTOS TREINTA Y UN PESOS M/CTE (\$421.337.621)**, equivalente a 11833, (UVT) Unidad de Valor Tributario, por la violación a lo dispuesto en:

- i. El literal a) del artículo 17, en concordancia con el literal d) del artículo 4 de la Ley 1581 de 2012, y con el artículo 2.2.2.25.4.3 del Decreto Único Reglamentario 1074 de 2015;
- ii. El literal b) del artículo 17, en concordancia con el literal b) del artículo 4, el literal a) del artículo 12 de la Ley 1581 de 2012, así como el inciso primero del artículo 2.2.2.25.2.2 del Decreto Único Reglamentario 1074 de 2015;
- iii. El literal c) del artículo 17, en concordancia con el literal b) del artículo 4, de la Ley 1581 de 2012;
- iv. El literal d) del artículo 17, en concordancia con el literal g) del artículo 4 de la Ley 1581 de 2012;
- v. El literal J) del artículo 17, en concordancia con el artículo 14 y el literal e) del artículo 4 de la Ley 1581 de 2012.
- vi. El literal j) del artículo 17, en concordancia con el artículo 15 de la Ley 1581 de 2012; y,
- vii. El literal o) del artículo 17 de la Ley 1581 de 2012.

**CUARTO:** Que en el término legal establecido para el efecto<sup>1</sup>, mediante escrito radicado con el número 18-26450-34 de 7 de septiembre de 2020 el apoderado general de **CREDIVALORES** (en adelante el **RECURRENTE**), interpuso recurso de reposición y en subsidio de apelación contra la Resolución No. 46328 de 11 de agosto de 2020, con fundamento en los siguientes argumentos:

#### **FUNDAMENTOS**

La Superintendencia de Industria y comercio por medio de Resolución 46328 de 2020 del 11 AGOSTO 2020, sanciona a mí representada por varios motivos, entre otros por faltar al "deber de solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular".

(...)

Respecto a esta valoración le informo al despacho que mi representada si cumple con la obligación enmarcada en la ley transcrita ya que conserva la autorización otorgada por el consumidor, autorización que me permito allegar con la presente y en captura de **pantalla**.



<sup>1</sup> Conforme con la constancia suscrita por la Coordinadora del Grupo de Notificaciones y Certificaciones de esta Superintendencia, radicada en el sistema de trámites bajo el número 18-26450-35 del 15 de septiembre de 2020, la Resolución 46328 del 11 de agosto de 2020 fue notificada por aviso a **CREDIVALORES** el 25 de agosto de 2010, con lo cual el término para presentar los recursos vencía el 8 de septiembre de 2020.

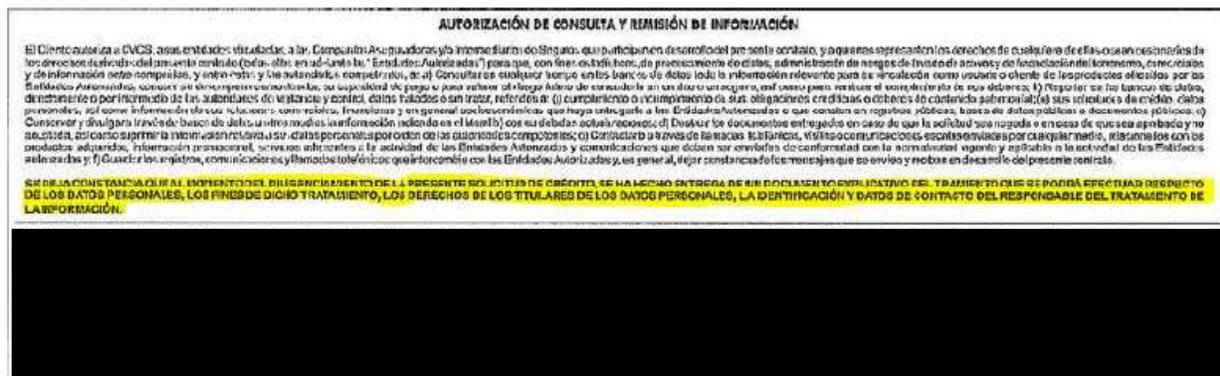
“Por la cual se resuelve un recurso de apelación”

VERSIÓN PÚBLICA

Por lo anteriormente [sic] expuesto le solicitó [sic] muy respetuosamente se reponga y revoque el numeral 8.2.2 de la resolución 46328 DE [sic] 2020 del [sic] 11 AGOSTO [sic] 2020, toda vez que como se demuestra mi representada no vulnera la normatividad, toda vez que conserva la autorización [sic] dada por la denunciante.

Así mismo [sic], el despacho determino [sic] que mi representada violo [sic] el “deber de informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización [sic] otorgada”.

Se le indica al despacho que al momento de la recolección de los datos demográficos de la denunciante se cumplió con esta obligación normativa, y se le informo [sic] a la misma, la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada, como se evidencia en la presente captura de pantalla y documento que allego con la presente:



Por lo anteriormente [sic] expuesto le solicitó [sic] muy respetuosamente se reponga y revoque el numeral 8.2.3 de la resolución 46328 DE [sic] 2020 del [sic] 11 AGOSTO [sic] 2020, toda vez que como se demuestra mi representada no vulnera la normatividad.

Por último el despacho arguye que mi representada vulnero [sic] “deber de tramitar las consultas formuladas en los términos señalados en la presente ley.”.

Al respecto me permito contradecir lo indicado por el despacho toda vez que mi representada si [sic] le dio tramite a los reclamos de la denunciante, como se indica en la misma investigación; el 27 de octubre de 2017 con oficio 2693599 y el 11 de diciembre [sic] de 2017 con oficio 2726758 CREDIVALORES S.A, les dio respuesta a los requerimientos de la denunciante incluso aceptando el error cometido. Por tanto, su señoría [sic] solicito se reponga y revoque el numeral 8.2.5 de la resolución 46328 DE 2020 [sic] del 11 AGOSTO 2020.

**QUINTO:** Que mediante Resolución 69299 de 29 de octubre de 2020, el Director de Investigación de Protección de Datos Personales resolvió el recurso de reposición interpuesto por **CREDIVALORES**, contra la Resolución 46328 de 11 de agosto de 2020, en los siguientes términos:

“**ARTÍCULO PRIMERO: REVOCAR** el ARTÍCULO PRIMERO de la Resolución 46328 del [sic] 11 de agosto de 2020 respecto de la sanción impuesta por lo dispuesto en:

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

**ARTÍCULO SEGUNDO: MODIFICAR** el ARTÍCULO PRIMERO de la Resolución 46328 del [sic] 11 de agosto de 2020, así:

**ARTÍCULO PRIMERO: IMPONER** una sanción pecuniaria a la sociedad **CREDIVALORES - CREDISERVICIOS S.A.**, identificada con NIT 805.025.964-3 de **TRESCIENTOS SIETE MILLONES DOSCIENTOS DIECISIETE MIL CIENTO NOVENTA Y SEIS PESOS M/CTE (\$307.217.196)**, equivalente a 8.628 (UVT) Unidad de Valor Tributario, por la violación a lo dispuesto en:

- i. El literal a) del artículo 17, en concordancia con el literal d) del artículo 4 de la Ley 1581 de 2012, y con el artículo 2.2.2.25.4.3 del Decreto Único Reglamentario 1074 de 2015;
- ii. El literal d) del artículo 17, en concordancia con el literal g) del artículo 4 de la Ley 1581 de 2012;
- iii. El literal j) del artículo 17, en concordancia con el artículo 14 y el literal e) del artículo 4 de la Ley 1581 de 2012.

iv. El literal j) del artículo 17, en concordancia con el artículo 15 de la Ley 1581 de 2012; y,

v. El literal o) del artículo 17 de la Ley 1581 de 2012".

**SEXTO:** Que de conformidad con lo establecido en el artículo 80 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, este Despacho procede a resolver el recurso de apelación interpuesto contra la Resolución 46328 del [sic] 11 de agosto de 2020, de conformidad con las siguientes,

#### CONSIDERACIONES DEL DESPACHO:

### 1. FUNCIONES DEL DESPACHO DEL SUPERINTENDENTE DELEGADO PARA LA PROTECCIÓN DE DATOS PERSONALES.

El artículo 16 del Decreto 4886 de 26 de diciembre de 2011<sup>2</sup> establece las funciones del Superintendente Delegado para la Protección de Datos Personales, entre las cuales se destacan las siguientes:

"(...)

7. Decidir los recursos de reposición y las solicitudes de revocatoria directa que se interpongan contra los actos que expida, así como los de apelación que se interpongan contra los actos expedidos por la Dirección a su cargo.

(...)"

### 2. DEBER OBTENER Y CONSERVAR LA AUTORIZACIÓN PREVIA OTORGADA POR EL TITULAR

El Artículo 15 de la Constitución Política, establece que "Todas las personas tienen derecho a (...) conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas". Así mismo ordena que en la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

En desarrollo del citado mandato constitucional, el literal b) del artículo 17 de la Ley 1581 de 2012 ordena lo siguiente

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

b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular;

En línea con lo anterior, el artículo 2.2.2.25.2.5 del Decreto 1074 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo", dispone 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.

Igualmente, el Responsable del Tratamiento le corresponde demostrar que ha cumplido la ley tal y como lo dispone el capítulo del citado Decreto 1074 de 2015:

**Artículo 2.2.2.25.6.1. Demostración.** Los Responsables del tratamiento de **datos personales** deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este capítulo (...) (Énfasis añadido)

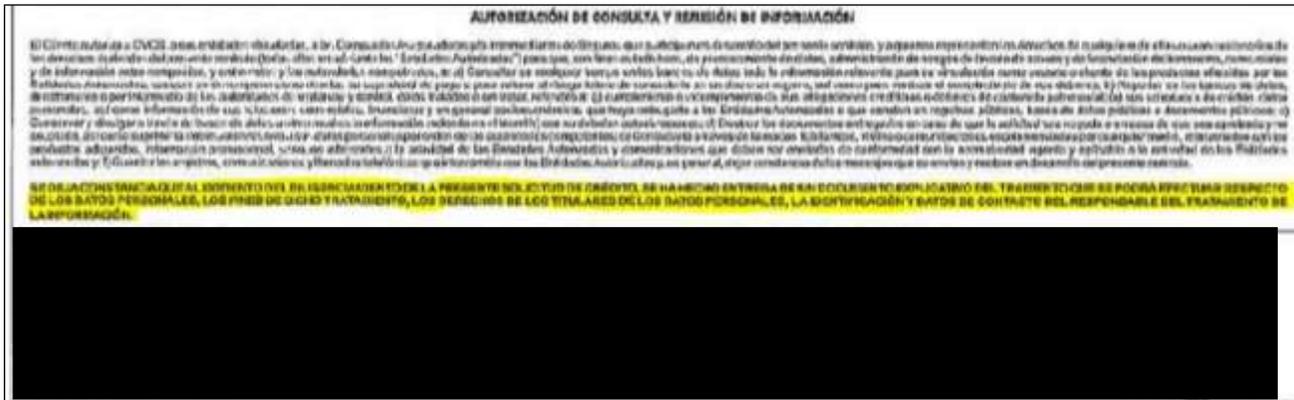
En suma, el Responsable del Tratamiento tiene la carga probatoria de, entre otras, acreditar la prueba obtenida para tratar los Datos del Titular.

Así las cosas, en el recurso de apelación el **RECORRENTE** da a conocer una captura de pantalla de la Autorización que diera la quejosa para el Tratamiento de sus Datos personales,

<sup>2</sup> Por medio del cual se modifica la estructura de la Superintendencia de Industria y Comercio, se determinan las funciones de sus dependencias y se dictan otras disposiciones.

“Por la cual se resuelve un recurso de apelación”

VERSIÓN PÚBLICA



Al respecto, la Dirección de Investigación de Protección de Datos Personales, al resolver el recurso de reposición, dispuso lo siguiente:

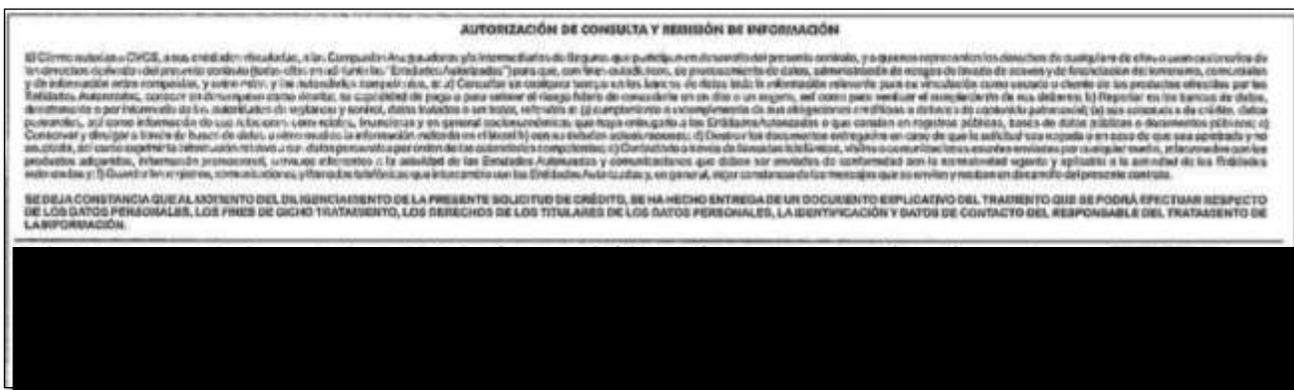
“Así las cosas, luego de examinadas las pruebas aportadas por la investigada con el recurso de reposición para desvirtuar el incumplimiento del “Deber de solicitar y conservar en las condiciones previstas en la Ley, copia de la respectiva autorización otorgada por el Titular”, esta Dirección concluye lo siguiente:

1. La sociedad **CREDIVALORES-CREDISERVICIOS S.A.** tenía la prueba para demostrar el cumplimiento de este deber, pero no la aportó durante la investigación a pesar de que en todas las etapas procesales esta Dirección le garantizó el derecho de defensa y contradicción. Por lo tanto, la investigada no fue diligente en presentar oportunamente las pruebas pertinentes para que fuesen consideradas antes de proferir la resolución recurrida.
2. Luego de transcurridos los términos procesales en los cuales la investigada guardó silencio, esta Dirección profirió su decisión con base en el acervo probatorio obrante en el expediente, teniendo como consecuencia la imposición de una sanción pecuniaria de **SETENTA MILLONES DOSCIENTOS DIECISIETE MIL CUATRO PESOS M/CTE (70.217.004)**, equivalente a 1972 (UVT) Unidad de Valor Tributario, por incumplir con el deber establecido en el literal b) del artículo 17, en concordancia con el literal c) del artículo 4, y el artículo 9 de la Ley 1581 de 2012, así como el artículo 2.2.2.25.2.2 del Decreto Único Reglamentario 1074 de 2015, toda vez que no acreditó prueba de la autorización [sic] previa, expresa e informada de la señora [REDACTED].
3. Verificadas las pruebas aportadas frente con [sic] los requisitos legales, se encuentra que la autorización [sic] suscrita por la Titular [REDACTED] fue otorgada con el consentimiento previo, expreso e informado.

Por lo tanto, esta Dirección encuentra que la sociedad **CREDIVALORES-CREDISERVICIOS S.A.**, cumplió con el literal b) del artículo 17, en concordancia con el literal c) del artículo 4 y el artículo 9 de la Ley 1581 de 2012, así como el inciso primero del artículo 2.2.2.25.2.2 del Decreto Único Reglamentario 1074 de 2015. **En consecuencia, se revoca la sanción impuesta y en su lugar, se ordena el archivo de la actuación respecto del cargo. (Destacamos)”**

Este Despacho, después de verificar las pruebas que fueron allegadas por parte del **RECURRENTE** con el recurso de apelación, coincide con lo dispuesto por la primera instancia cuando revocó la sanción impuesta por no cumplir con el literal b) del artículo 17 de la Ley 1581 de 2012.

Efectivamente, al verificar la solicitud de crédito allegada por el **RECURRENTE** en el escrito de apelación encontró lo siguiente:



De la anterior imagen puede leerse lo siguiente:

El Cliente autoriza a CVCS, a sus entidades vinculadas, a las Compañías Aseguradoras y/o intermediarios de Seguros que participen en desarrollo del presente contrato, y a quienes representen los derechos de cualquiera de estas o sean cesionarios de los derechos derivados del presente contrato (todas en adelante

las “Entidades Autorizadas”) para que, con fines estadísticos, de procesamiento de datos, administración de riesgos de lavado de activos y de financiación del terrorismo, comerciales y de información entre compañías, y entre éstas y las autoridades competentes, a: a) Consultar en cualquier tiempo en los bancos de datos toda la información relevante para su vinculación como usuario o cliente de los productos ofrecidos por las Entidades Autorizadas conocer su desempeño como deudor, su capacidad de pago o para valorar el riesgo futuro de concederle un crédito o un seguro, así como para verificar el cumplimiento de sus deberes; b) Reportar en los bancos de datos, directamente o por intermedio de las autoridades de vigilancia y control, datos tratados o sin tratar, referidos a: (1) cumplimiento o incumplimiento de sus obligaciones crediticias o deberes de contenido patrimonial; (2) sus solicitudes de crédito, datos personales, así como información de sus relaciones comerciales, financieras y en general socioeconómicas que haya entregado a las Entidades Autorizadas o que consten en registros públicos, bases de datos públicas o documentos públicos; c) Conservar y divulgar a través de bases de datos u otros medios la información indicada en el literal b) con sus debidas actualizaciones; d) Destruir los documentos entregados en caso de que la solicitud sea negada o en caso de que se aprobada y no aceptada, así como suprimir la información relativa a sus datos personales por orden las autoridades competentes; e) Contactarlo a través de llamadas telefónicas, visitas o comunicaciones escritas enviadas por cualquier medio, relacionados con los productos adquiridos, información promocional, servicios inherentes a la actividad de las Entidades Autorizadas y comunicaciones que deban ser enviadas de conformidad con la normatividad vigente y aplicable de las Entidades autorizadas y; f) Guardar los registros, comunicaciones y llamadas telefónicas que intercambie con las entidades Autorizadas y, en general, dejar constancia de los mensajes que se envíen y reciban en desarrollo del presente contrato.

SE DEJA CONSTANCIA QUE EL MOMENTO DEL DILIGENCIAMIENTO DE LA PRESENTE SOLICITUD, SE HA HECHO ENTREGA DE UN DOCUMENTO EXPLICATIVO DEL TRATAMIENTO QUE SE PODRÁ EFECTUAR RESPECTO DE LOS DATOS PERSONALES, LOS FINES DE DICHO TRATAMIENTO, LOS DERECHOS DE LOS TITULARES DE LOS DATOS PERSONALES, LA IDENTIFICACIÓN Y DATOS DE CONTACTO DEL RESPONSABLE DEL TRATAMIENTO DE LA INFORMACIÓN.

Así las cosas, y en la medida que el **RECURRENTE** a partir de las pruebas allegadas logra desvirtuar el cargo formulado y por el cual fue sancionada **CREDIVALORES** relacionado en el literal b) del artículo 17, en concordancia con el literal c) del artículo 4 y el artículo 9 de la Ley 1581 de 2012, así como el inciso primero del artículo 2.2.2.25.2.2 del Decreto Único Reglamentario 1074 de 2015; y el literal c) del artículo 17, en concordancia con el literal b) del artículo 4, el literal a) del artículo 12 de la Ley 1581 de 2012, así como el inciso primero del artículo 2.2.2.25.2.2 del Decreto Único Reglamentario 1074 de 2015, razón por la cual este Despacho comparte la decisión proferida por la primera instancia en la Resolución 69299 de 29 de octubre de 2020, cuando revocó la sanción impuesta por la vulneración de las normas relacionadas.

### 3. DEBER DE RESOLVER CONSULTAS Y RECLAMOS FORMULADAS POR EL TITULAR DEL DATO PERSONAL.

Manifestó el **RECURRENTE** lo siguiente

*“Por último el despacho arguye que mi representada vulnero “deber de tramitar las consultas formuladas en los términos señalados en la presente ley.”.*

*Al respecto me permito contradecir lo indicado por el despacho toda vez que mi representada si le dio tramite a los reclamos de la denunciante, como se indica en la misma investigación; el 27 de octubre de 2017 con oficio 2693599 y el 11 de diciembre de 2017 con oficio 2726758 CREDIVALORES S.A, les dio respuesta a los requerimientos de la denunciante incluso aceptando el error cometido. Por tanto, su señoría solicito se reponga y revoque el numeral 8.2.5 de la resolución 46328 DE2020 del 11 AGOSTO 2020”.*

Considera este Despacho oportuno señalar la importancia del derecho de petición respecto del ejercicio del derecho de *habeas data*, contemplado en el artículo 15 de la Constitución Política.

El artículo 17 literal j) de la Ley 1581 de 2012, dispone lo siguiente:

*“Artículo 17. Deberes de los Responsables del Tratamiento. Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:*

*(...)*

*j) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley”.* (Negrilla fuera de texto)

*(...)*

En desarrollo de lo anterior, los artículos 14 y 15 regulan el procedimiento que debe seguirse respecto de los reclamos, así:

**“ARTÍCULO 14. CONSULTAS.** Los Titulares o sus causahabientes podrán consultar la información personal del Titular que repose en cualquier base de datos, sea esta del sector público o privado. El Responsable del Tratamiento o Encargado del Tratamiento deberán suministrar a estos toda la información contenida en el registro individual o que esté vinculada con la identificación del Titular.

La consulta se formulará por el medio habilitado por el Responsable del Tratamiento o Encargado del Tratamiento, siempre y cuando se pueda mantener prueba de esta.

La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

**PARÁGRAFO.** Las disposiciones contenidas en leyes especiales o los reglamentos expedidos por el Gobierno Nacional podrán establecer términos inferiores, atendiendo a la naturaleza del dato personal”.

**“ARTÍCULO 15. RECLAMOS.** El Titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en esta ley, podrán presentar un reclamo ante el Responsable del Tratamiento o el Encargado del Tratamiento el cual será tramitado bajo las siguientes reglas:

1. El reclamo se formulará mediante solicitud dirigida al Responsable del Tratamiento o al Encargado del Tratamiento, con la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

2. Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga “reclamo en trámite” y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

3. El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término”.

La Corte Constitucional mediante la Sentencia T-814 de 2005 precisó que el derecho de petición “conlleva la posibilidad de que las personas puedan dirigirse a las autoridades públicas u organizaciones privadas, en interés particular o general con el fin de presentar solicitudes respetuosas y esperar una respuesta clara y precisa del asunto presentado a su consideración en el término legalmente establecido. En virtud de lo anterior, la esencia del derecho de petición comprende algunos elementos: **(i) pronta resolución, (ii) respuesta de fondo, (iii) notificación de la respuesta al interesado**”. (negrilla fuera de texto).

Asimismo, en la Sentencia T-129 de 2010 señaló que, “(l)a relación de los derechos al buen nombre y hábeas data con el derecho fundamental de petición resulta inescindible en la medida que este último se transforma en el mecanismo idóneo para la materialización de los dos primeros”. En consecuencia, la materialización de los derechos al buen nombre y hábeas data, mediante el ejercicio del derecho de petición, implica que se dé una respuesta de fondo y oportuna de acuerdo con los términos señalados en la ley y sea notificada al interesado<sup>3</sup>.

Por su parte, mediante la Sentencia C-748 de 6 de octubre de 2011 respecto del artículo 14 transcrito, manifestó lo siguiente:

<sup>3</sup> Cfr. Corte Constitucional, Sentencia T-350 de 2006. M.P. Jaime Cordoba Triviño. “La jurisprudencia constitucional de esta Corporación ha señalado que el núcleo esencial del derecho de petición comprende los siguientes elementos o características: (i) la posibilidad cierta y efectiva de presentar, de manera respetuosa, solicitudes ante las autoridades, sin que éstas se nieguen a recibir las o se abstengan de tramitarlas; (ii) la facultad de obtener una respuesta oportuna, esto es, dentro de los términos previstos en el ordenamiento jurídico; (iii) el derecho a recibir una respuesta de fondo o contestación material, lo que supone que la autoridad analice la materia propia de la solicitud y se pronuncie sobre la totalidad de los asuntos planteados, es decir, la correspondencia entre la petición y la respuesta, excluyendo fórmulas evasivas o elusivas y; (iv) la pronta comunicación al peticionario sobre la determinación adoptada, con independencia de que su contenido sea favorable o desfavorable. Si no se cumple con estos requisitos se incurre en una vulneración del derecho fundamental de petición”.

**"Esta norma hace una regulación típica del derecho de petición que consagra el artículo 23 de la Constitución tanto en el inciso primero como en el segundo, por cuanto el primero señala que todas las personas tienen derecho a presentar peticiones respetuosas ante las autoridades por motivos de interés general o particular, hecho que en el caso en estudio se traduce en el derecho que tienen los titulares del habeas data o sus causahabientes para presentar ante los bancos de datos que manejen las autoridades públicas, peticiones para establecer qué información o datos poseen sobre ellos.**

**En el segundo inciso del mencionado artículo 23 señala que el legislador podrá reglamentar su ejercicio ante organizaciones privadas para garantizar los derechos fundamentales. Es precisamente esta regulación la que hace el artículo 14, al estipular que los responsables y/o encargados del tratamiento de datos, en este caso los privados, deben atender en los precisos términos las consultas que eleven ante ellos los titulares del derecho al habeas data, como una forma de hacer exigibles el derecho consagrado en el literal a) del artículo 8 del proyecto en revisión, específicamente el de conocer.**

**En este orden de ideas, el derecho de petición que se regula en la norma objeto de análisis se convierte en un instrumento con el que cuenta el titular del dato para hacer exigible o realizable el derecho autónomo de habeas data. Es por ello que la jurisprudencia constitucional ha definido el derecho de petición como un derecho instrumental a través del cual el ciudadano se acerca a la administración o a aquellos privados que en razón de la actividad que desarrollan ostentan una posición de privilegio sobre el resto de particulares, que obliga al Estado a regular mecanismos que le permitan a estos últimos tener una herramienta que los obligue a responder a las inquietudes e inconformidades que se puedan generar por razón de la actividad que éstos desplieguen, en procura de lograr la satisfacción de otros derechos fundamentales.**

**En ese sentido, el legislador estatutario al regular de forma general la protección del dato personal, estaba facultado para señalar los términos en que los responsables y encargados del tratamiento del dato, públicos y privados, deben responder las consultas o peticiones que les eleve el titular del dato o sus causahabientes, con el fin de hacer exigibles entre otros, el derecho a conocer qué datos personales tiene un determinado banco de datos y la forma como éstos son manejados. Compatible con esto, los artículos 17, literal k) y 18 literal f) del proyecto, establecen como uno de los deberes del responsable y encargado del tratamiento del dato, el de adoptar un manual interno de políticas y procedimiento especialmente para la atención de las consultas y reclamos por parte de los titulares. Igualmente, como una forma de lograr un mayor conocimiento por parte del titular de las bases de datos que operan en el país y cuáles pueden estar tratando su información, el proyecto crea el registro nacional de bancos de datos, artículo 25, el cual será objeto de análisis posteriormente.**

**En consecuencia, el precepto revisado resulta ajustado a la Constitución. No obstante, la Sala debe advertir que la jurisprudencia constitucional<sup>272</sup> 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". (Negrilla fuera de texto)**

Por lo tanto, no responder de manera respetuosa, **completa y de fondo**, dentro del término legal establecido, un reclamo o solicitud hecha por un Titular de información, **vulnera su derecho fundamental de habeas data**, impidiendo que **conozca**, actualice o rectifique la **información que sobre él se tenga en una Base de Datos o archivo**.

Anexo a la queja presentada por la señora [REDACTED], está el derecho de petición presentado ante **CREDIVALORES** el 18 de octubre de 2017, y en el que solicitó:

**"... por favor necesito que me envíen una copia de los datos y correos PERSONALES que tienen ya que llegó un extracto a una persona que no tengo contacto hace años. La tarjeta la adquirí aproximadamente hace un AÑO. COMO ES POSIBLE QUE ESTAS COSAS SUCEDAN. ESTA ES UNA INFORMACIÓN QUE DEBE LLEGAR ÚNICA Y EXCLUSIVAMENTE solo a mí."**

Como respuesta a la anterior consulta, **CREDIVALORES** dio respuesta mediante oficio de 26 de octubre de 2017, en los siguientes términos:

➤ **RESPUESTA A SU PETICIÓN:**

**Actualización de datos demográficos:** De acuerdo a su petición se procedió a realizar la actualización de sus datos personales en nuestro sistema de acuerdo al artículo 8 de la ley estatutaria 1581 de 2012 en la cual usted como titular de sus datos personales tiene el derecho de "Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento en este caso Credivalores - Crediservicios S.A.S. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado".

Le ofrecemos nuestras más sinceras disculpas por los inconvenientes que esta situación le haya generado y le reiteramos la disposición permanente de Credivalores - Crediservicios S.A.S para continuar ofreciéndole el mayor y más oportuno respaldo, invitándole a que se comunique con nosotros cada vez que sienta que el servicio entregado no coincide con sus expectativas.

La presente contestación se envía por medio electrónico conforme a lo establecido en el artículo 56 de la ley 1437 de 2011 y a la Sentencia 25000233600020140032801 del 28 de julio de 2014, proferida por la Sección Quinta del Consejo de Estado, toda vez que en el Derecho de Petición radicado por usted con fecha 18 de Octubre de 2017, se relacionó el correo [nataliariarcosmartinez@gmail.com](mailto:nataliariarcosmartinez@gmail.com)

En espera de haber dado respuesta a sus pretensiones, agradecemos la atención prestada y cualquier inquietud con gusto será atendida a través de nuestras líneas de Servicio al Cliente 482 32 82 en Bogotá y 01 8000 950 303 para el resto del país, mediante nuestras redes sociales Facebook: [Credivalores - Crediservicios S.A.S](#), Twitter: [@Crediconsultas](#) o si lo prefiere en la página web [www.credivalores.com.co](http://www.credivalores.com.co) – link contáctenos.

Ahora bien, y en la medida que la respuesta dada por **CREDIVALORES** no resolvió de fondo la solicitud de información hecha por la quejosa, el 5 de diciembre de 2017, presentó un nuevo derecho de petición en los siguientes términos:

**PETICIONES**

**PRIMERO:** Solicito cordialmente me sea informado de que fuente adquirieron datos de otras personas para suministrarle mi información relacionada con los servicios que tengo con ustedes.

**SEGUNDO:** En atención a la petición anterior, solicito que dichos datos sean eliminados y suprimidos teniendo en cuenta que no corresponden a la suscrita.

Como respuesta a lo anterior, **CREDIVALORES**, informó:

➤ **RESPUESTA A SU PETICIÓN:**

En virtud de lo manifestado en su comunicación con respecto al tratamiento de sus datos personales nos permitimos reiterar la información enviada a su dirección de correo electrónico el pasado 26 de Octubre del presente año en el cual se procedió a realizar la actualización de sus datos personales y se dio alcance a su solicitud radicada bajo número de requerimiento 2693599 con fecha 20 de Octubre de 2017.

Dicho lo anterior, debido a un cruce en nuestras bases de datos se originaron envíos de comunicaciones a un correo diferente al establecido por usted, no obstante, se procedió a generar la respectiva actualización para que este tipo de situaciones no se vuelvan a presentar y toda comunicación sea enviada al correo [nataliariarcosmartinez@gmail.com](mailto:nataliariarcosmartinez@gmail.com)

Nuevamente, le ofrecemos nuestras más sinceras disculpas por los inconvenientes que esta situación le haya generado y le reiteramos la disposición permanente de Credivalores - Crediservicios S.A.S para continuar ofreciéndole el mayor y más oportuno respaldo, invitándole a que se comunique con nosotros cada vez que sienta que el servicio entregado no coincide con sus expectativas.

La presente contestación se envía por medio electrónico conforme a lo establecido en el artículo 56 de la ley 1437 de 2011 y a la Sentencia 25000233600020140032801 del 28 de julio de 2014, proferida por la Sección Quinta del Consejo de Estado, toda vez que en el Derecho de Petición radicado por usted con fecha 05 de Diciembre de 2017, se relacionó el correo [nataliariarcosmartinez@gmail.com](mailto:nataliariarcosmartinez@gmail.com)

Como se observa, CREDIVALORES no respondió lo específicamente preguntado por la Titular del dato en el numeral primero porque no le informó de qué fuente adquirió datos de otras personas para suministrarles información de ella respecto de los servicios contratados con dicha empresa.

Adicionalmente, la Titular se vio obligada a radicar dos (2) derechos de peticiones porque CREDIVALORES no respondió de manera completa y de fondo lo requerido.

Este Despacho ha sido enfático en determinar que:

***“No puede convertirse en práctica empresarial que el titular del dato tenga que insistir varias veces para que se garantice el respeto de sus derechos. Con una sola solicitud es suficiente y le corresponde al Responsable hacer efectivo el derecho de las personas dentro de los plazos máximos legales establecidos en la ley. Los derechos de los titulares son para respetarlos en el tratamiento de datos personales y no para dilatar su cumplimiento o negar su efectividad en la práctica.”***<sup>4</sup> (Destacamos)

Conforme con lo solicitado por la quejosa en su reclamo y la respuesta recibida por parte de **CREDIVALORES**, es claro para este Despacho que también se vulneraron las normas de protección de Datos por cuanto respecto de la supresión de información solicitada guardó silencio y **remitió nuevamente el extracto de la tarjeta de crédito a un correo electrónico desconocido por la quejosa.**

En virtud de lo anterior, CREDIVALORES no garantizó a la Titular el pleno y efectivo ejercicio del derecho de hábeas data. Tampoco tramitó ni respondió debidamente las consultas y reclamos formulados en los términos señalados en la Ley Estatutaria 1581 de 2012.

#### **4. DEL PRINCIPIO Y DEL DEBER DE SEGURIDAD EN EL DEBIDO TRATAMIENTO DE DATOS PERSONALES.**

Sin seguridad no existe debido tratamiento de datos personales. Es por eso que la regulación señala, entre otras, lo siguiente:

##### **Literal g) Artículo 4 de la Ley 1581 de 2012:**

*La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.*

##### **Literal d) Artículo 17 de la Ley 1581 de 2012:**

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

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

La relevancia y alcance del deber de seguridad ha sido puesto de presente en los siguientes términos:

*“La seguridad es un proceso dinámico en constante evolución y prueba. Se quiere que exista un nivel de seguridad apropiado en las diferentes etapas del tratamiento de datos personales en donde las medidas de seguridad sean objeto de evaluación y revisión.*

*Dichas medidas deben estar enfocadas para mitigar los siguientes riesgos: acceso no autorizado a los datos personales, pérdida, destrucción (accidental o no autorizada),*

<sup>4</sup> Cfr. Resolución 83882 del 15 de noviembre de 2018 de la Superintendencia de Industria y Comercio

*contaminación (por virus informático) uso fraudulento, consulta, copia, modificación, adulteración, revelación, comunicación, o difusión no autorizados.*

*Para establecer las medidas se deben tener en cuenta, entre otras, las técnicas de seguridad existentes en general y para sectores específicos, los riesgos que presente el tratamiento y la naturaleza de los datos que deban protegerse, la probabilidad y severidad del daño obtenido, la sensibilidad de la información y el contexto en el que es realizado el tratamiento y las eventuales consecuencias negativas para los titulares de los datos. (...)*

*Proteger la información es una condición crucial del tratamiento de datos personales. Una vez recolectada debe ser objeto de medidas de diversa índole para evitar situaciones indeseadas que pueden afectar los derechos de los titulares y de los mismos Responsables y Encargados del tratamiento de los datos. El acceso, la consulta y el uso no autorizado o fraudulento así como la manipulación y pérdida de la información son los principales riesgos naturales y humanos que se quieren mitigar a través de medidas de seguridad de naturaleza humana, física, administrativa o técnica.”<sup>5</sup>*

Por su parte, la Corte Constitucional ha establecido que:

*“Al amparo de este principio, 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.*

*(..)*

***Existe entonces un deber tanto de los Responsables como los Encargados de establecer controles de seguridad, de acuerdo con el tipo de base de datos que se trate, que permita garantizar los estándares de protección consagrados en esta Ley Estatutaria.”<sup>6</sup>*** (Subrayado fuera de texto).

En el presente caso, la recurrente no cumplió el deber y el principio de seguridad porque suministró a terceros datos personales de la Titular del datos. En otras palabras, no adoptó las medidas de seguridad necesarias para impedir el acceso no autorizado de esos datos. Al contrario, lo que hizo la recurrente fue facilitar el acceso no autorizado al remitir comunicaciones a terceros con información personal de la Titular.

Así, este Despacho procederá a confirmar la decisión contenida en la Resolución 46328 de 11 de agosto de 2020, y que fuera revocada parcialmente por la Resolución 69299 de 29 de octubre de 2020.

## **5. RESPONSABILIDAD DEMOSTRADA (ACCOUNTABILITY) Y “COMPLIANCE” EN EL TRATAMIENTO DE DATOS PERSONALES**

La regulación colombiana le impone al Responsable del Tratamiento la responsabilidad de garantizar la eficacia de los derechos del Titular del Dato, la cual no puede ser simbólica ni formal, sino real y demostrable. Téngase presente que según nuestra jurisprudencia “existe un deber constitucional de administrar correctamente y de proteger los archivos y Bases de Datos que contengan información personal o socialmente relevante”<sup>7</sup>.

Adicionalmente, los Responsables o Encargados del Tratamiento no son dueños de los datos personales que reposan en sus Bases o archivos. En efecto, ellos son meros tenedores que están en el deber de administrar de manera correcta, apropiada y acertada la información de las personas porque su negligencia o dolo en esta materia afecta los derechos humanos de los Titulares de los Datos.

En virtud de lo anterior, el capítulo III del Decreto 1377 de 27 de junio de 2013 -incorporado en el Decreto 1074 de 2015- reglamenta algunos aspectos relacionados con el principio de responsabilidad demostrada.

<sup>5</sup> Cfr. REMOLINA ANGARITA, Nelson. 2013. Tratamiento de datos personales: aproximación internacional y comentarios a la ley 1581 de 2012. 1 ed. Bogotá: Legis Editores. Págs. 216-217

<sup>6</sup> Corte Constitucional. Sentencia C – 748 del 2011.

<sup>7</sup> Cfr. Corte Constitucional, Sentencia T-227 de 2003

El artículo 26<sup>8</sup> -titulado DEMOSTRACIÓN- establece que *“los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012”*. Así, resulta imposible ignorar la forma en que el Responsable o Encargado del Tratamiento debe probar poner en funcionamiento medidas adecuadas, útiles y eficaces para cumplir la regulación. Es decir, se reivindica que un administrador no puede utilizar cualquier tipo de políticas o herramientas para dicho efecto, sino solo aquellas que tengan como propósito lograr que los postulados legales sean realidades verificables, y no solo se limiten a creaciones teóricas e intelectuales.

Es de resaltar que la Corte Constitucional mediante la sentencia C-32 de 2021 reconoció la existencia de la responsabilidad demostrada en los siguientes términos:

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

***El principio de responsabilidad demostrada, de acuerdo con lo expuesto, consiste en el deber jurídico del responsable del tratamiento de demostrar ante la autoridad de datos que cuenta con la institucionalidad y los procedimientos para garantizar las distintas garantías***

<sup>8</sup> El texto completo del artículo 26 del Decreto 1377 de 2013 ordena lo siguiente: Artículo 26. Demostración. Los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este decreto, en una manera que sea proporcional a lo siguiente:

1. La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.
2. La naturaleza de los datos personales objeto del tratamiento.
3. El tipo de Tratamiento.
4. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares.

En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, los Responsables deberán suministrar a esta una descripción de los procedimientos usados para la recolección de los datos personales, como también la descripción de las finalidades para las cuales esta información es recolectada y una explicación sobre la relevancia de los datos personales en cada caso. En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, quienes efectúen el Tratamiento de los datos personales deberán suministrar a esta evidencia sobre la implementación efectiva de las medidas de seguridad apropiadas”

*del derecho al habeas data, en especial, la vigencia del principio de libertad y las facultades de conocimiento, actualización y rectificación del dato personal.”<sup>9</sup> (Destacamos)*

Con el propósito de dar orientaciones sobre la materia, la Superintendencia de Industria y Comercio expidió el 28 de mayo de 2015 la “Guía para implementación del principio de responsabilidad demostrada (*accountability*)”<sup>10</sup>.

El término “*accountability*” a pesar de los diferentes significados ha sido entendido en el campo de la protección de datos como el modo en que una organización debe cumplir (en la práctica) las regulaciones sobre el tema, y la manera en que debe demostrar que lo puesto en práctica es útil, pertinente y eficiente.

Conforme con ese análisis, las recomendaciones que trae la guía a los obligados a cumplir la ley 1581 de 2012:

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

El principio de responsabilidad demostrada –*accountability*– demanda implementar acciones de diversa naturaleza<sup>11</sup> para garantizar el correcto cumplimiento de los deberes que imponen las regulaciones sobre Tratamiento de Datos personales. El mismo, exige que los Responsables y Encargados del Tratamiento implementen medidas apropiadas, efectivas y verificables que le permitan evidenciar la observancia de las normas sobre la materia.

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

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

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

En este sentido, desde el año 2006 la Red Iberoamericana de Protección de Datos (RIPD) ha puesto de presente que “la autorregulación sólo redundará en beneficio real de las personas en la medida que sea bien concebida, aplicada y cuente con mecanismos que garanticen su cumplimiento de manera que **no se constituyan en meras declaraciones simbólicas de buenas intenciones sin que produzcan efectos concretos en la persona cuyos derechos y libertades pueden ser lesionados o amenazados por el tratamiento indebido de sus datos personales**”<sup>12</sup> (Destacamos).

El principio de responsabilidad demostrada busca que los mandatos constitucionales y legales sobre Tratamiento de Datos personales sean una realidad verificable y redunden en beneficio de la protección de los derechos de las personas. Por eso, es crucial que los administradores de las

<sup>9</sup> Cfr. Corte Constitucional, sentencia C-032 del 18 de febrero de 2021. M.P. Dra Gloria Stella Ortiz. El texto de la sentencia puede consultarse en: <https://www.corteconstitucional.gov.co/relatoria/2021/C-032-21.htm>

<sup>10</sup> El texto de la guía puede consultarse en: <http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf>

<sup>11</sup> Estas medidas pueden ser de naturaleza administrativa, organizacional, estratégica, tecnológica, humanas y de gestión que involucran procesos y procedimientos.

<sup>12</sup> Cfr. Red Iberoamericana de Protección de Datos. Grupo de trabajo temporal sobre autorregulación y protección de datos personales. Mayo de 5 de 2006. En aquel entonces, la RIPD expidió un documento sobre autorregulación y protección de datos personales que guarda cercana relación con “*accountability*” en la medida que la materialización del mismo depende, en gran parte, de lo que internamente realicen las organizaciones y definan en sus políticas o regulaciones internas.

organizaciones sean proactivos respecto del Tratamiento de la información de manera que por iniciativa propia adopten medidas estratégicas capaces de garantizar los derechos de los Titulares de los Datos personales y su gestión siempre sea respetuosa de los derechos humanos.

Aunque no es espacio para explicar cada uno de los anteriores aspectos mencionados en la guía<sup>13</sup>, ponemos de presente que el principio de responsabilidad demostrada se articula con el concepto de "compliance" en la medida que este hace referencia al "conjunto de procedimientos y buenas prácticas adoptados por las organizaciones para identificar y clasificar los riesgos operativos y legales a los que se enfrentan y establecer mecanismos internos de prevención, gestión, control y reacción frente a los mismos"<sup>14</sup>.

También se ha afirmado que "compliance es un término que hace referencia a la gestión de las organizaciones conforme a las obligaciones que le vienen impuestas (requisitos regulatorios) o que se ha autoimpuesto (éticas)"<sup>15</sup>. Adicionalmente se precisa que "ya no vale solo intentar cumplir" la ley sino que las organizaciones "deben asegurarse que se cumple y deben generar evidencias de sus esfuerzos por cumplir y hacer cumplir a sus miembros, bajo la amenaza de sanciones si no son capaces de ello. Esta exigencia de sistemas más eficaces impone la creación de funciones específicas y metodologías de compliance"<sup>16</sup>.

Por tanto, las organizaciones deben "implementar el compliance" en su estructura empresarial con miras a acatar las normas que inciden en su actividad y demostrar su compromiso con la legalidad. Lo mismo sucede con "accountability" respecto del Tratamiento de Datos personales.

La identificación y clasificación de riesgos, así como la adopción de medidas para mitigarlos son elementos cardinales del compliance y buena parte de lo que implica el principio de responsabilidad demostrada (accountability). En la mencionada guía se considera fundamental que las organizaciones desarrollen y pongan en marcha, entre otros, un "sistema de administración de riesgos asociados al tratamiento de datos personales"<sup>17</sup> que les permita "identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos en desarrollo del cumplimiento de las normas de protección de datos personales"<sup>18</sup>.

## 6. RESPONSABILIDAD DE LOS ADMINISTRADORES EN MATERIA DE TRATAMIENTO DE DATOS PERSONALES.

El artículo 2 de la Constitución de la República de Colombia de 1991 señala que son fines esenciales del Estado, entre otros, "garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución". De aquí se desprende la exigencia de obtener resultados positivos y concretos del conjunto de disposiciones mencionadas. En este caso en particular, del derecho constitucional a la protección de datos previsto en el artículo 15 superior.

La efectividad de los derechos humanos es un asunto de gran importancia en la sociedad a tal punto que es una exigencia de naturaleza constitucional y del más alto nivel en el ordenamiento jurídico. Por eso, el artículo 2 continúa ordenando a las "autoridades de la República están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias, y demás derechos y libertades, y para asegurar el cumplimiento de los deberes sociales del Estado y de los particulares".

Las normas que hablan de la protección de Datos en el sentido que se estudia, deben ser interpretadas de manera armónica con el ordenamiento jurídico del cual hacen parte y sobre todo con su Constitución Política. Así, su artículo 333 establece que "la actividad económica y la iniciativa privada son libres, dentro de los límites del bien común". Este "bien común" se refiere a cuestiones relevantes para una sociedad como, entre otros, la protección de los derechos humanos porque son imprescindibles para que cualquier ser humano sea tratado como una "persona" y no como un objeto o cosa.

<sup>13</sup> El texto de la guía puede consultarse en: <http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf>

<sup>14</sup> Cfr. World Compliance Association (WCA). <http://www.worldcomplianceassociation.com/> (última consulta: 6 de noviembre de 2018)

<sup>15</sup> Cfr. Bonatti, Francisco. Va siendo hora que se hable correctamente de compliance (III). Entrevista del 5 de noviembre de 2018 publicada en Canal Compliance: <http://www.canal-compliance.com/2018/11/05/va-siendo-hora-que-se-hable-correctamente-de-compliance-iii/>

<sup>16</sup> Idem

<sup>17</sup> Cfr. Superintendencia de Industria y Comercio (2015) "Guía para implementación del principio de responsabilidad demostrada (accountability)". Págs 16-18

<sup>18</sup> Ibid. P 16

En línea con lo anterior, nuestra Carta Política recalca que la “libre competencia económica es un derecho de todos que supone responsabilidades” y que la “empresa, como base del desarrollo, tiene una función social que implica obligaciones”. Como se observa, la actividad empresarial no puede realizarse de cualquier manera y en el mundo empresarial no tiene cabida jurídica la afirmación según la cual el “fin justifica los medios”. En efecto, no se trata de una libertad ilimitada, sino de una actividad “restringida” porque no solo debe ser respetuosa del bien común, sino que demanda el cumplimiento de obligaciones constitucionales y legales.

El bien común a que se refiere el precitado artículo 333 mencionado, exige que la realización de cualquier actividad económica garantice, entre otras, los derechos fundamentales de las personas. Es por eso que la Constitución Política pone de presente que la participación en el mercado supone responsabilidades y que efectuar actividades empresariales implica cumplir con las obligaciones previstas en la ley.

Ahora, según el artículo 22 de la Ley 222 de 1995<sup>19</sup> la expresión administradores comprende al *“representante legal, el liquidador, el factor, los miembros de juntas o consejos directivos y quienes de acuerdo con los estatutos ejerzan o detenten esas funciones”*. Cualquiera de ellos tiene la obligación legal de garantizar los derechos de los Titulares de los Datos y de cumplir la Ley 1581 de 2012 y cualquier otra norma concordante. Por esto, el numeral segundo del artículo 23 de la Ley 222 de 1995 determina que los administradores deben *“obrar de buena fe, con lealtad y con la diligencia de un buen hombre de negocios”*, y además, en el ejercicio de sus funciones deben ***“velar por el estricto cumplimiento de las disposiciones legales o estatutarias”***. (Destacamos)

En vista de lo anterior, la regulación no exige cualquier tipo de cumplimiento de la ley, sino uno calificado. Es decir, ajustado o con exactitud a lo establecido en la norma. Velar por el estricto cumplimiento de la ley exige que los administradores actúen de manera muy profesional, diligente y proactiva para que en su organización la regulación se cumpla de manera real y no formal con la efectividad y rigurosidad requeridas.

Por eso, los administradores deben cuidar al detalle y con perfecta seguridad este aspecto. No basta solo con ser guardianes, deben ser promotores de la correcta y precisa aplicación de la ley. Esto, desde luego, los obliga a verificar permanentemente si la ley se está o no cumplimiento en todas las actividades que realiza su empresa u organización.

El artículo 24<sup>20</sup> de la Ley 222 de 1995, presume la culpa del administrador “en los casos de incumplimiento o exlimitación de sus funciones, violación de la ley o de los estatutos”. Dicha presunción de responsabilidad exige que los administradores estén en capacidad de probar que han obrado con lealtad y la diligencia de un experto. Es decir, como un “buen hombre de negocios”, tal y como lo señala su artículo 23.

Adicionalmente, no debe perderse de vista que los administradores responden “solidaria e ilimitadamente de los perjuicios que por dolo o culpa ocasionen a la sociedad, a los socios o a terceros”<sup>21</sup>. Las disposiciones referidas, prevén unos elementos de juicio ciertos, (i) *el alto nivel de responsabilidad jurídica y económica en cabeza de los administradores*, y (ii) *el enorme profesionalismo y diligencia que debe rodear su gestión en el tratamiento de datos personales*.

<sup>19</sup> Ley 222 de 1995 “Por la cual se modifica el Libro II del Código de Comercio, se expide un nuevo régimen de procesos concursales y se dictan otras disposiciones”

<sup>20</sup> El texto completo del artículo 24 de la ley 222 de 1995 dice lo siguiente: “Artículo 24. RESPONSABILIDAD DE LOS ADMINISTRADORES. El artículo 200 del Código de Comercio quedará así:

*Artículo 200. Los administradores responderán solidaria e ilimitadamente de los perjuicios que por dolo o culpa ocasionen a la sociedad, a los socios o a terceros.*

*No estarán sujetos a dicha responsabilidad, quienes no hayan tenido conocimiento de la acción u omisión o hayan votado en contra, siempre y cuando no la ejecuten.*

*En los casos de incumplimiento o exlimitación de sus funciones, violación de la ley o de los estatutos, se presumirá la culpa del administrador.*

*De igual manera se presumirá la culpa cuando los administradores hayan propuesto o ejecutado la decisión sobre distribución de utilidades en contravención a lo prescrito en el artículo 151 del Código de Comercio y demás normas sobre la materia. En estos casos el administrador responderá por las sumas dejadas de repartir o distribuidas en exceso y por los perjuicios a que haya lugar.*

*Si el administrador es persona jurídica, la responsabilidad respectiva será de ella y de quien actúe como su representante legal.*

*Se tendrán por no escritas las cláusulas del contrato social que tiendan a absolver a los administradores de las responsabilidades antedichas o a limitarlas al importe de las cauciones que hayan prestado para ejercer sus cargos.”*

<sup>21</sup> Cfr. Parte inicial del artículo 24 de la ley 222 de 1995

En virtud de todo lo anterior se exhorta al Representante Legal de **CREDIVALORES – CREDISERVICIOS S.A.** para que adopte medidas pertinentes, útiles, efectivas y verificables con miras a:

- a) Respetar y garantizar los derechos de los Titulares de los Datos;
- b) Evitar que se repitan hechos como los que dieron origen a la presente investigación;
- c) Dar estricto cumplimiento de las disposiciones legales y estatutarias sobre Tratamiento de Datos personales;
- d) Aplicar el principio de responsabilidad demostrada, observando las orientaciones de la Superintendencia de Industria y Comercio incorporadas en la "Guía para implementación del principio de responsabilidad demostrada (accountability)"<sup>22</sup>. Especial énfasis se debe hacer en utilizar mecanismos de monitoreo y control que permitan comprobar la efectividad de las medidas adoptadas para responder las consultas y reclamos de los Titulares de los Datos.
- e) Garantizar la seguridad en el tratamiento de datos personales.

## 7. CONCLUSIONES.

Sin perjuicio de lo establecido, no se accederá a las pretensiones de la RECURRENTE, por, entre otras, las siguientes razones:

- a) **CREDIVALORES** en el recurso de apelación únicamente manifestó su inconformidad respecto de los cargos relacionados con la Autorización previa y la respuesta de consultas y reclamos, guardando silencio sobre los demás cargos sancionados, incluyendo sobre el valor de la sanción impuesta.
- b) La Dirección de Investigación de Protección de Datos Personales al resolver el recurso de reposición, revocó parcialmente la decisión contenida en la Resolución 46328 de 11 de agosto de 2020, en la medida que **CREDIVALORES** logró probar la existencia de la Autorización previa para el Tratamiento de los Datos personales, otorgada por la quejosa. Por esa razón, la multa se redujo en un 27% respecto del monto inicial.
- c) **CREDIVALORES** no dio respuesta, completa y de fondo a los derechos de petición presentados por la quejosa. Por ende, **CREDIVALORES** no garantizó a la Titular el pleno y efectivo ejercicio del derecho de hábeas data. Tampoco tramitó ni respondió debidamente las consultas y reclamos formulados en los términos señalados en la Ley Estatutaria 1581 de 2012.
- d) La Titular se vio obligada a radicar dos (2) derechos de peticiones porque **CREDIVALORES** no respondió de manera completa y de fondo lo requerido. Este Despacho ha sido enfático en determinar que: *"No puede convertirse en práctica empresarial que el titular del dato tenga que insistir varias veces para que se garantice el respeto de sus derechos. Con una sola solicitud es suficiente y le corresponde al Responsable hacer efectivo el derecho de las personas dentro de los plazos máximos legales establecidos en la ley. Los derechos de los titulares son para respetarlos en el tratamiento de datos personales y no para dilatar su cumplimiento o negar su efectividad en la práctica."* (Destacamos)
- e) Sin seguridad no existe debido tratamiento de datos personales. En el presente caso, **CREDIVALORES** no cumplió el deber y el principio de seguridad porque suministró a terceros datos personales de la Titular del dato. En otras palabras, no adoptó las medidas de seguridad necesarias para impedir el acceso no autorizado de esos datos.

De conformidad con lo indicado y una vez analizadas las pruebas y documentos allegados a la presente actuación administrativa, encuentra este Despacho que la resolución objeto de impugnación fue expedida observando la ley. De esta forma y de acuerdo con el artículo 80 del Código de Procedimiento Administrativo y lo Contencioso Administrativo y las consideraciones del Despacho, se confirmará la Resolución 46328 de 11 de agosto de 2020, que fuera revocada parcialmente por la Resolución 69299 de 29 de octubre de 2020.

<sup>22</sup> El texto de la guía puede consultarse en: <http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf>

En mérito de lo expuesto, este Despacho,

### RESUELVE

**ARTÍCULO PRIMERO:** Confirmar en todas sus partes la Resolución 46328 de 11 de agosto de 2020, revocada parcialmente por la Resolución 69299 de 29 de octubre de 2020, de conformidad con lo expuesto en la parte motiva del presente acto administrativo.

**ARTÍCULO SEGUNDO:** Exhortar a la Representante Legal de **CREDIVALORES – CREDISERVICIOS S.A. ELIANA ANDREA ERAZO RESTREPO**, C.C. 52.189.858 para que adopte las medidas pertinentes, útiles, efectivas y verificables con miras a:

- a) Respetar y garantizar los derechos de los Titulares de los Datos;
- b) Evitar que se repitan hechos como los que dieron origen a la presente investigación;
- c) Dar estricto cumplimiento de las disposiciones legales y estatutarias sobre Tratamiento de Datos personales.
- d) Aplicar el principio de responsabilidad demostrada, observando las orientaciones de la Superintendencia de Industria y Comercio incorporadas en la “Guía para implementación del principio de responsabilidad demostrada (accountability)”<sup>23</sup>. Especial énfasis se debe hacer en utilizar mecanismos de monitoreo y control que permitan comprobar la efectividad de las medidas adoptadas para responder las consultas y reclamos de los Titulares de los Datos personales.
- e) Garantizar la seguridad en el tratamiento de los datos personales.

**ARTÍCULO TERCERO:** Notificar personalmente el contenido de la presente decisión a la **CREDIVALORES – CREDISERVICIOS S.A.** identificada con el NIT 805.025.964-3, a través de su representante legal o apoderado, entregándole copia de la misma e informándole que contra el presente acto administrativo no procede recurso alguno.

**ARTÍCULO CUARTO:** Comunicar la presente decisión a la señora [REDACTED], identificada con la cédula de ciudadanía [REDACTED].

**ARTÍCULO QUINTO:** Informar el contenido de la presente resolución al Director de Investigación de Protección de Datos Personales y devolverle el expediente para su custodia final.

### NOTIFÍQUESE, COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá, D.C., agosto 03 de 2021

**El Superintendente Delegado para la Protección de Datos Personales,**

**NELSON REMOLINA ANGARITA**

NTL

<sup>23</sup> El texto de la guía puede consultarse en: <http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf>

**NOTIFICACIÓN:**

Sociedad: **CREIVALORES – CREDISERVICIOS S.A.**  
Identificación: Nit. 805.025.964-3  
Representante legal: **ELIANA ANDREA ERAZO RESTREPO**  
Identificación: C.C. 52.189.858  
Dirección: Carrera 7 No. 76-35 Piso 7  
Ciudad: Bogotá D.C.  
Correo electrónico: [impuestos@creivalores.com](mailto:impuestos@creivalores.com)

**COMUNICACIÓN:****Titular de la Información:**

Señora: [REDACTED]  
Identificación: C.C. [REDACTED]  
Dirección: [REDACTED]  
Ciudad: [REDACTED]  
Correo Electrónico: [REDACTED]