

Cartillas Cámara
6/2020



**UNIVERSIDAD
DE ANTIOQUIA**

Facultad de Derecho y Ciencias Políticas



**CAMARA DE COMERCIO®
DE MEDELLIN PARA ANTIOQUIA**



Guía práctica sobre protección de datos personales

**Guía práctica sobre protección de datos personales.
Una publicación de la Cámara de Comercio de Medellín para
Antioquia.**

Diciembre de 2020

Lina Vélez de Nicholls
Presidenta Ejecutiva

Jorge Villegas Betancur
Secretario General y Vicepresidente Jurídico

Autora:

Ángela María Lozada García
Semillero de investigación en Derecho, Tecnología e Innovación
de la Facultad de Derecho y Ciencias Políticas de la Universidad
de Antioquia.

Equipo técnico:

Liliana María Castillo Restrepo
Directora Jurídica

Natalia Isaza Jaramillo
Jefe de Estudios Jurídicos

Alejandra Vélez Medina
Abogada Gestión Jurídica

Saray Marcela Bedoya Lozano
Abogada de Estudios Jurídicos

Coordinación editorial:

Vicepresidencia de Comunicaciones y Mercadeo

Edición y diagramación:

Marcela Hernández Sanzón y Blanco Contenido

Los contenidos de esta publicación son propiedad de la Cámara de Comercio de Medellín para Antioquia, su reproducción total o parcial sin autorización expresa del titular está prohibida. Todos los derechos reservados ©.

Calle 53 # 45-77, Medellín.

1. Introducción

Actualmente, el comercio electrónico juega un papel fundamental en la sociedad y las empresas están volcando su mirada al mundo digital para transformar su negocio. Por este motivo, la Cámara de Comercio de Medellín para Antioquia y la Universidad de Antioquia diseñaron esta cartilla para contribuir al entendimiento de los aspectos más relevantes de la Ley 1581 de 2012 y del Decreto 1377 de 2013 (compilado en el Decreto 1074 de 2015) sobre el tratamiento y protección de datos personales y, de esta forma, poder implementar algunas pautas y actividades para un adecuado tratamiento de los datos en el ámbito del comercio electrónico dentro de las organizaciones.

Nota aclaratoria: El contenido de esta cartilla es material informativo que les permitirá a los comerciantes iniciar el programa corporativo de protección de datos personales. Sin embargo, como responsables del tratamiento de datos personales, es tarea exclusiva de los comerciantes cumplir a cabalidad con los requisitos establecidos en la normativa.

2. ¿A qué se refiere la protección de datos personales?

Las empresas, al realizar sus actividades comerciales u operativas, emplean una serie de datos de clientes, empleados, proveedores o de cualquier sujeto que suministre información personal, por lo que deben tener un especial cuidado para no poner en riesgo la seguridad de dicha información ni exponerse a potenciales sanciones de ley por no cumplir con la normativa, viendo afectada su imagen y reputación. Deben ser conscientes de que los datos personales que administran no les pertenecen y que tienen la responsabilidad de hacer un tratamiento adecuado de los mismos, velando siempre por la confidencialidad, integridad y disponibilidad de la información.

3. ¿Qué se entiende por datos personales?

Cuando se habla de datos personales se hace referencia a toda información asociada a una persona y que permite su identificación. Por ejemplo, su documento de identidad, el lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral, o profesional. Existe también información más sensible como su estado de salud, sus características físicas, ideología política, vida sexual, entre otros aspectos (Superintendencia de Industria y Comercio (SIC)).

Entonces, los datos personales se pueden entender como cualquier información que identifique a una persona, que tenga carácter privado, que se encuentre relacionado con la intimidad y que pueda llegar a generar discriminación si se dan a conocer. Por ejemplo, señales particulares, número

GUÍA PRÁCTICA SOBRE PROTECCIÓN DE DATOS PERSONALES

telefónico, dirección, correo electrónico, aficiones, datos de localización (GPS), dirección de protocolo de internet (IP), información de salud, orientación sexual, orientación política, origen étnico, filiación religiosa, color de piel, etc.

La Ley de Protección de Datos Personales los clasifica en 4 categorías de acuerdo con el nivel de riesgo si se llegara a divulgar el dato:

Las definiciones de estos conceptos se encuentran estable-

DATOS PÚBLICOS

Son datos que facilitan el contacto con la sociedad.

Pueden circular de manera libre.

DATOS SEMIPRIVADOS

Son los datos cuyo conocimiento solo puede interesar al titular de los datos y a cierto sector o grupo de personas.

DATOS PRIVADOS

Son datos que facilitan el contacto con la sociedad. Son los de naturaleza íntima o reservada como fotos, gustos, aficiones, dirección de residencia, teléfono privado, correo electrónico personal, etc.

Pueden circular de manera libre.

DATOS SENSIBLES

Son los datos que si se conocen podrían afectar al titular porque pueden causar discriminación, por ejemplo, su orientación sexual, filiación política, estado de salud, datos biométricos, etc.

cidas en el artículo 3 de la Ley 1581 de 2012; en el artículo 3 del Decreto 1377 de 2013 compilado en el Decreto 1074 de 2015, y en el artículo 3 de la Ley 1266 de 2008.

4. ¿Por qué es importante esta clasificación?

La clasificación de los datos sirve porque en el comercio electrónico se va a recolectar información y, antes de hacerlo, es necesario identificar qué datos se recopilarán y clasificarlos, para establecer si se debe solicitar autorización del titular, o no.

5. ¿En qué consiste la Ley de Protección de Datos Personales?

La Ley de Protección de Datos Personales o Ley 1581 de 2012 y Decreto Reglamentario 1377 de 2013 (compilado en el capítulo 25 del Decreto 1074 de 2015, Único Reglamentario del Sector Comercio, Industria y Turismo (DUR)) busca proteger los derechos con los que cuentan todas las personas naturales como titulares de los datos personales. Estos son, por ejemplo, conocer y actualizar la información que se haya recolectado sobre ellas y, en caso de requerirlo, rectificarla y solicitar la supresión de los datos personales que se encuentren almacenados en las bases de datos o archivos, tanto físicos como digitales.

Por su parte, el Decreto Reglamentario 1377 de 2013 (compilado en el Decreto 1074 de 2015) facilita el cumplimiento y la implementación de los mecanismos relativos al tratamiento de datos personales establecidos en la Ley 1581 de 2012.



Ley 1581 de 2012.
Decreto Reglamentario 1377 de 2013.
Decreto Reglamentario 1074 de 2015.

6. ¿Quiénes están obligados a cumplir con esta normativa?

Esta normativa busca que todas las personas naturales o jurídicas y a quienes les sea aplicable la legislación colombiana en virtud de normas y tratados internacionales, realicen un adecuado tratamiento de los datos personales de terceros, respetando los principios, derechos, garantías y procedimientos previstos en la ley.

7. ¿Qué tipo de bases de datos personales están exentos de esta normativa?

Las bases de datos y archivos a los que no les aplican estas disposiciones, según el artículo 2 de la Ley 1581 de 2012, son aquellos que:

- ▶ Son mantenidas en un ámbito exclusivamente personal o doméstico.
- ▶ Tienen por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo.
- ▶ Contienen y tienen como fin información de inteligencia y contrainteligencia.
- ▶ Información periodística y otros contenidos editoriales.
- ▶ Las reguladas por la Ley 1266 de 2008.
- ▶ Las reguladas por la Ley 79 de 1993.

8. ¿En qué consiste el tratamiento de datos personales?

Las empresas adquieren información de personas naturales y jurídicas por diferentes canales, por ejemplo, en la elaboración de las facturas, en encuestas, formularios, llamadas telefónicas, contacto a través de las páginas web, etc. Esta información es almacenada en las bases de datos de la empresa, sea en documentos físicos, archivos de Excel o bases de datos. Posteriormente, es utilizada para el objetivo que se recolectó y puede circular por diferentes áreas o personas dentro de la empresa como secretarías, facturación, nómina, etc., hasta que se archiva o se elimina.

Es muy importante conocer el ciclo de vida de los datos dentro del negocio, por qué áreas circulan y quiénes son las personas que pueden tener acceso a ellos de acuerdo con las finalidades que autorizaron los titulares.

Por lo tanto, se entiende como tratamiento de datos personales la recolección, almacenamiento, uso, circulación, análisis, indexación y supresión, en otras palabras, la gestión de la información al interior del negocio.

9. Ciclo de vida de los datos



La Organización para la Cooperación y el Desarrollo Económicos (OCDE) (2016) ha recomendado:

“Las empresas deberían proteger los datos personales del consumidor, asegurándose de que sus prácticas relacionadas con la recopilación y el uso de datos del consumidor sean legales, transparentes y justas, y que permitan la participación y elección del consumidor y tomen precauciones de seguridad razonables”.

10. ¿Quiénes participan en el tratamiento de datos personales?



Cuando se vayan a compartir con terceros bases de datos o archivos que contengan datos personales, de manera previa se deberá solicitar la autorización a cada uno de los titulares e informar la finalidad para la cual se comparte dicha información.



En este caso, tanto el responsable como el encargado de las bases de datos y archivos deberán cumplir con las disposiciones contenidas en la ley.

II. ¿Qué derechos tiene el titular de los datos personales?

El titular de los datos personales tiene los siguientes derechos que se encuentran consagrados en el artículo 8 de la Ley 1581 de 2012:



12. ¿Qué sanciones se pueden imponer por el incumplimiento de la norma?

La SIC, como ente de inspección, control y vigilancia, tiene competencia para investigar las conductas contrarias a la ley que afecten los derechos de las personas, así como para imponer sanciones a los responsables y encargados del tratamiento.

En el artículo 23 de la Ley 1581 de 2012 se encuentran establecidas estas sanciones:

- ▶ Multas de carácter personal o institucional hasta por 2000 salarios mínimos mensuales legales vigentes (SMMLV).
- ▶ Suspensión de las actividades relacionadas con el tratamiento de datos personales hasta por seis meses.
- ▶ Cierre temporal de las operaciones relacionadas con el tratamiento de datos personales si no se adoptaron los correctivos ordenados en el acto de suspensión.
- ▶ Cierre definitivo de las operaciones que impliquen tratamiento de datos sensibles de las personas.

13. ¿Cuáles son las conductas que representan mayores sanciones?

- ▶ Adquirir bases de datos piratas o ilegales.
- ▶ Fallas en la seguridad de la información.
- ▶ No solicitar o no conservar la autorización a los titulares.
- ▶ No informar al titular la finalidad del tratamiento.
- ▶ Entregar las bases de datos a terceros sin la autorización de los titulares.
- ▶ No recibir las peticiones o no atender los reclamos o solicitudes en los términos de ley.
- ▶ No adoptar políticas de tratamientos de datos personales.

14. ¿Cuándo se vulneran los derechos de los titulares asociados a la protección de datos?

01 Cuando los datos personales sean tratados para fines distintos para los que fueron recolectados.

02 Cuando rebasen la esfera de privacidad.

03 Cuando no se actualizan.

04 Cuando no se toman medidas para garantizar la seguridad.

05 Cuando se entregan a terceros sin autorización del titular.



15. ¿Cómo puede ejercer el titular su derecho a la protección de datos?



01 Presentar un reclamo ante el responsable o el encargado del tratamiento

02 Si no se recibe una respuesta o si la que se recibe es inadecuada (plazo de 15 días hábiles para atender la reclamación, contados a partir del día siguiente a la fecha de su recibo).

03 El reclamo se eleva ante la SIC.

16. ¿Qué deben tener presentes el responsable y el encargado?

- ▶ Garantizarle al titular, durante todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- ▶ Solicitar, de manera previa al tratamiento, la autorización del titular y conservar copia respectiva.
- ▶ Almacenar la información bajo medidas de seguridad para impedir su modificación, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- ▶ Dar respuesta a las consultas y reclamos formulados por los titulares en los tiempos establecidos por la SIC.
- ▶ Implementar políticas y un manual de procedimientos para garantizar el adecuado tratamiento de datos personales.
- ▶ Capacitar al personal permanentemente sobre la importancia de la protección de los datos personales.
- ▶ Cumplir las indicaciones y requerimientos impartidos por la SIC.

17. Puntos claves para cumplir con la protección de datos personales

FINALIDAD

Tener clara la finalidad que se le darán a los datos.

Deben ser datos realmente necesarios.

RECOLECCIÓN DEL DATO PERSONAL

Solicitar y conservar autorización dada por el titular.

INFORMACIÓN CLARA

Informar de manera oportuna y clara la finalidad de la recolección de los datos.

TRATAMIENTO Y CIRCULACIÓN

Informar finalidad, disposición y derechos frente a los datos.

TRAMITAR

Las consultas y reclamos realizados por el titular de los datos o su representante.

SEGURIDAD INFORMACIÓN

Garantizarles a los titulares la seguridad digital y física de los datos.

CAPACITAR

Mantener actualizado y capacitar al personal sobre la protección de datos personales.
Poner a disposición políticas y manuales para consulta.

GESTIONAR LOS DATOS

Contar con los procedimientos de actualización, supresión y rectificación oportuna cuando el titular lo solicite.

18. Listado de ítems que se deben tener presentes dentro de la documentación

Este es un listado informativo que no especifica toda la documentación necesaria debido a que esta depende de las circunstancias propias de cada empresa u organización:

DOCUMENTO/PRODUCTO	SÍ	NO
Inventario de los fines de la recolección de los datos		
Inventario de los canales de comunicación a través de los cuales los titulares pueden ejercer sus derechos ante el responsable y/o encargado del tratamiento		
Política de tratamiento de datos personales		
Políticas de <i>cookies</i>		
Manual de procedimientos de protección de datos personales		
Formato autorización para el tratamiento de datos personales		
Formato de revocatoria y supresión		
Aviso de privacidad		
Aviso legal en la sección “Contáctenos” de la página web		
Aviso legal en el formulario PQRS		
Aviso legal en la suscripción a boletines electrónicos		
Aviso legal en el chat		
Aviso legal en el formulario de transmisión de datos personales a la plataforma de pagos		
Flujograma: <ul style="list-style-type: none"> ▶ Procedimiento de consultas del dato ▶ Procedimiento para la revocatoria del dato ▶ Procedimiento para supresión del dato 		

19. Autorización otorgada por el titular

Es el consentimiento previo, expreso e informado que otorga cualquier persona para que las empresas o responsables del tratamiento de la información puedan utilizar sus datos personales.

Es importante tener presente que el responsable del tratamiento deberá adoptar procedimientos para solicitar, a más tardar en el momento de la recolección de sus datos, la autorización del titular para el tratamiento de los mismos e informarle cuáles serán los datos personales recolectados, así como todas las finalidades específicas del tratamiento para las que se obtiene el consentimiento.

Los medios más comunes para recolectar la autorización son: escrito, verbal, correo electrónico, cámaras de video, dispositivos electrónicos o conductas inequívocas del titular que permiten concluir, de forma razonable, que otorgó la autorización.



Formatos modelo para el cumplimiento de obligaciones establecidas en la Ley 1581 de 2012 y sus derechos reglamentarios:

https://www.sic.gov.co/centro-de-publicaciones?-field_tema_general_tid=5&field_anos_p_value=All

20. ¿Qué debe contener la autorización en las plataformas de comercio electrónico?

- ▶ El titular debe saber que no está obligado a autorizar el tratamiento.
- ▶ Identificar cuáles de los datos que se van a recolectar son de carácter sensible.
- ▶ Informar dónde puede consultar las políticas para el tratamiento de datos personales.
- ▶ El titular debe manifestar que la autorización le fue solicitada y puesta de presente antes de entregar los datos, y que la suscribió de forma libre y voluntaria una vez leída en su totalidad.
- ▶ Guardar el LOG de registro (registro secuencial de acciones o actividades que han ido interactuando con el sistema, se almacenan en un archivo en orden cronológico) – Validar usuario.

21. ¿Qué se entiende por finalidades?

Las finalidades de la recolección de datos personales son las razones u objetivos para los que son recolectados, en otras palabras, el porqué de la necesidad de acceder y almacenar esta información.

La recolección de datos personales debe tener una finalidad legítima y cierta, es decir, una razón de ser de esa recolección. Además, los datos recolectados deben ser pertinentes y adecuados para alcanzar dicho fin. Por ejemplo, si lo que la organización quiere es vincular un nuevo cliente al portafolio de su empresa, debe pensar si es necesario solicitar datos como su talla de ropa o de calzado cuando lo que se pretende es venderle productos para mascotas” (SIC).



Ejemplos de finalidades:

https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cartilla_formatos_datos_Personales_nov22.pdf

22. ¿Qué son las cookies?

Es un archivo creado por el sitio web que contiene datos del visitante y que se envía del servidor donde está alojado el sitio web al navegador que utiliza el usuario.

El propósito principal de este archivo es identificar y almacenar información de las personas que ingresan a la página web para brindarles una experiencia de compra más personalizada. Entre otros:

1. Las páginas que visita el usuario en el sitio web.
2. Información que identifica al usuario.
3. Información del dispositivo que emplea.
4. Información del navegador que utiliza para acceder al sitio web.
5. Información de la ubicación.
6. Historial de actividad en un sitio web.

23. ¿Qué es el aviso de privacidad?

Es la información que se les brinda a los titulares (puede ser verbal o escrita) para darles a conocer la existencia y las formas de acceder a las políticas de tratamiento de la información y el objetivo de su recolección y uso.

Los avisos de privacidad permiten afianzar el nivel de confianza entre los responsables y los titulares debido a que se presenta con antelación a las finalidades y transferencias a las que serán sometidos los datos una vez se recolecten.

24. Qué diferencia existe entre las políticas de tratamiento de datos personales y el manual de tratamiento de datos personales

Las políticas de tratamiento de datos personales es una hoja de ruta que comunica a los titulares de estos datos cómo los utiliza la empresa. Son las reglas de juego que se plasman en políticas y procedimientos que aplican en la empresa en donde se esclarece cuál será el uso o tratamiento que se les darán a los datos recolectados, cuáles son los derechos de los titulares y cómo puede ejercerlos, de manera que el titular, de forma previa, pueda decidir si desea otorgar o no la autorización para el tratamiento y, de esta manera, ejerza el control de su información personal.

Por su parte, el manual detalla los deberes y obligaciones de los encargados y responsables del tratamiento de datos personales; los derechos de los titulares, la seguridad de la información, el área responsable de atender las quejas y reclamos, y los procedimientos internos para atender peticiones, consultas y reclamos de los titulares, entre otros.

25. ¿Qué se debe tener presente para desarrollar las políticas de tratamiento de datos personales?

Los responsables y encargados del tratamiento de datos personales tienen la obligación de implementar políticas y procedimientos internos en los que se expliquen claramente todas las reglas que utilizará la empresa para garantizar el correcto tratamiento de los datos.

Al desarrollar estas políticas se busca establecer los criterios para la recolección, almacenamiento, uso, circulación y supresión de los datos personales tratados por su negocio. Se recomienda tener presente:



Ámbito de aplicación.



Definiciones.

Principios para el tratamiento de datos personales:

- ▶ Principio pertinencia.
- ▶ Protección especial a los datos sensibles.
- ▶ Principio de libertad.
- ▶ Principio de legalidad en materia de tratamiento de datos.
- ▶ Principio de finalidad.
- ▶ Principio de veracidad o calidad.
- ▶ Principio de transparencia.
- ▶ Principio de acceso y circulación restringida.
- ▶ Principio de seguridad.
- ▶ Principio de confidencialidad.
- ▶ Principio de temporalidad del dato.



TITULARES DE LOS DATOS

- ▶ Derechos que le asisten como titular de los datos.
- ▶ Tratamientos de datos personales de niñas, niños y adolescentes.



RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES

- ▶ Identificación del responsable del tratamiento de datos.
- ▶ Canales de atención.
- ▶ Deberes del responsable del tratamiento.





ENCARGADO DEL TRATAMIENTO DE DATOS PERSONALES

- ▶ Deberes de los encargados del tratamiento de datos personales.

TRATAMIENTO DE LOS DATOS PERSONALES

- ▶ Autorización y consentimiento del titular.
- ▶ Finalidades del tratamiento de los datos personales.
- ▶ Prohibiciones.
- ▶ Procedimiento para la atención de solicitudes.
 - ▶ Consultas.
 - ▶ Reclamos, corrección o actualización.
 - ▶ Supresión del dato.
 - ▶ Revocatoria de la autorización.
- ▶ Políticas cuando actúe en condición de encargado del tratamiento.
- ▶ Transferencias y transmisiones internacionales de datos personales.
- ▶ Temporalidad de la información.
- ▶ Entrega de datos personales a autoridades.
- ▶ Mecanismos de seguridad de la información.



- Versión.
- Vigencia de la política.



Modelo de política de tratamiento de datos personales:

https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cartilla_formatos_datos_Personales_nov22.pdf

26. ¿Cuáles procedimientos se deben tener presentes para la protección de datos personales?

Para el cumplimiento de la Ley 1581 de 2012 y del Decreto 1377 de 2013 (compilado en el Decreto 1074 de 2015) se deben implementar los procedimientos para brindar atención a las consultas, peticiones y reclamos que el titular puede realizar para ejercer su derecho de conocer, actualizar, rectificar, suprimir los datos o rectificar la autorización en los términos que la ley establece.

Consulta

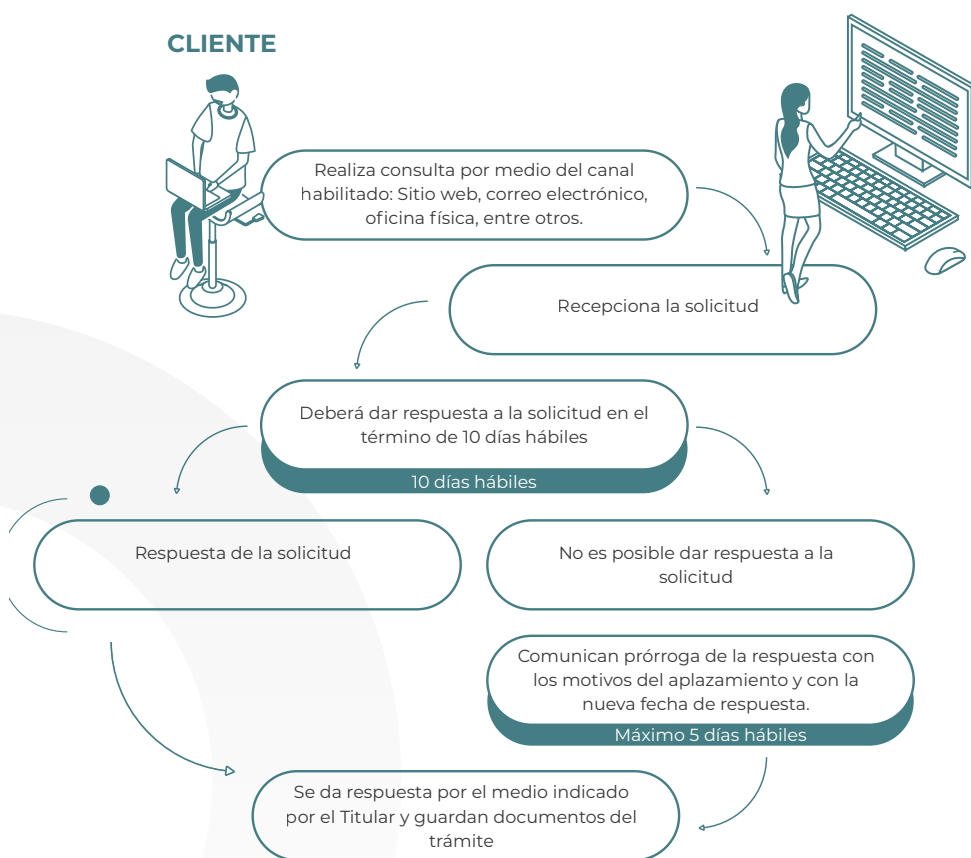
El titular, su causahabiente, tercero autorizado o apoderado podrán consultar la información personal que repose en cualquiera de las bases de datos de la empresa. Esta solicitud se puede realizar de forma escrita o verbal.

La consulta deberá ser atendida en un término máximo de 10 días hábiles contados a partir de la fecha de su recibo.



Cuando no sea posible atender la consulta dentro de ese término, se informará al interesado expresando los motivos de la demora y señalando la fecha en que se atenderá, la cual, en ningún caso, podrá superar los cinco días hábiles siguientes al vencimiento del primer término (artículo, Ley de 2012).

GUÍA PRÁCTICA SOBRE PROTECCIÓN DE DATOS PERSONALES



Reclamos, corrección o actualización

Para la atención del reclamo el empresario contará con un plazo máximo de 15 días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuera posible atenderlo dentro de dicho término, se le informarán los motivos de la demora y la nueva fecha de respuesta, la cual, en ningún caso, podrá superar los ocho días hábiles siguientes al vencimiento del primer término (artículo 15, Ley 1581 de 2012).



- ▶ Si la información de la solicitud está incompleta, el titular tendrá cinco días hábiles contados a partir del día siguiente a la fecha de recepción para que la complete.
- ▶ En caso de que el empresario no sea competente para resolver la solicitud, deberá dar traslado a quien corresponda en un término máximo de dos días hábiles, e informará de la situación al titular.

Supresión

El titular de los datos personales tiene derecho a solicitar la supresión (eliminación) total o parcial de sus datos personales contenidos en los registros, archivos y bases de datos tratados por el empresario cuando:



1. En el tratamiento de sus datos no se respeten los principios, deberes y garantías constitucionales y legales.
2. Hayan dejado de ser necesarios o pertinentes para la finalidad para la cual fueron recolectados.
3. Se haya superado el periodo necesario para el cumplimiento de los fines para los que fueron recolectados.

GUÍA PRÁCTICA SOBRE PROTECCIÓN DE DATOS PERSONALES

Es importante tener en cuenta que el derecho de supresión no es absoluto y que el responsable puede negarlo cuando:

- ▶ El titular tiene el deber legal o contractual de permanecer en la base de datos.
- ▶ La eliminación de datos obstaculice actuaciones judiciales o administrativas.
- ▶ Los datos sean necesarios para proteger los intereses jurídicamente tutelados del titular.



Datos mínimos:

- Identificación del titular o del tercero facultado legalmente.
- Descripción de los hechos.
- Dirección.
- Documentos.



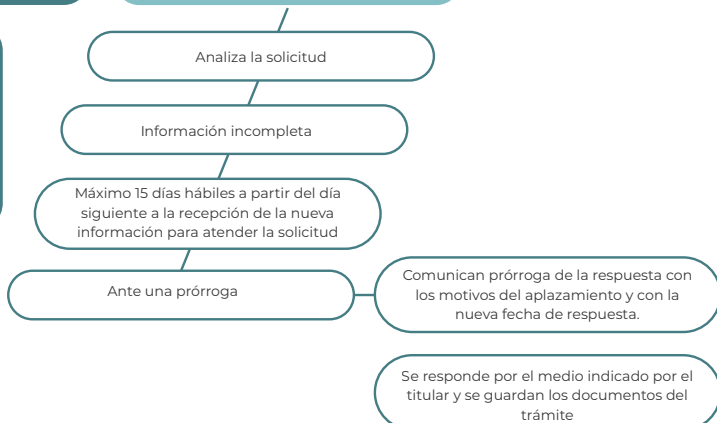
TITULAR

Envía la información solicitada

- ### Datos mínimos:
- Identificación del titular o del tercero facultado legalmente.
 - Descripción de los hechos.
 - Dirección.
 - Documentos.

RESPONSABLE

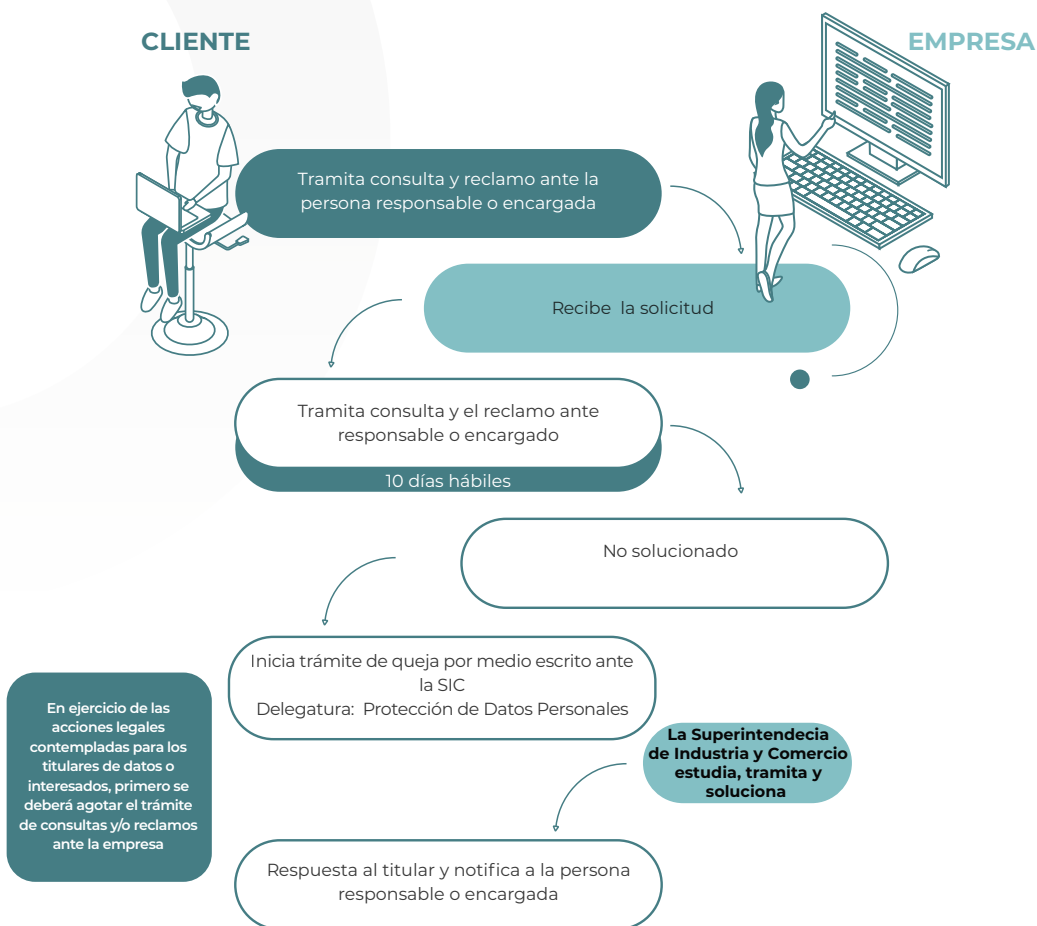
Recibe la nueva información



27. Revocatoria de la autorización

Cuando no exista una obligación legal o contractual que le imponga al titular el deber de permanecer en una base de datos de acuerdo con lo establecido en el artículo 15 de la Ley 1581 de 2012, este podrá solicitar al responsable o encargado la supresión de sus datos personales y/o revocar la autorización otorgada para el tratamiento de los mismos presentando un reclamo en virtud de la solicitud libre y voluntaria.

28. Procedimiento ante la SIC



29. Recomendaciones para el sitio de comercio electrónico

01

Cuando el proyecto de comercio electrónico tiene impacto en varios países o utiliza datos de personas ubicadas en diferentes partes del mundo, **se deben cumplir las normas locales sobre tratamiento de datos personales.**

02

Implementar las políticas y procedimientos internos sobre protección de datos personales.

03

Recolectar los datos estrictamente necesarios para fines de comercio electrónico.

04

Exigir el respeto de la política de tratamiento de datos personales a los terceros que contrata para realizar actividades de comercio electrónico.

05

Tener presente la privacidad de los consumidores desde el diseño del sitio de comercio electrónico.

06

Realizar las validaciones pertinentes para evitar la suplantación de identidad de los consumidores.

07

Evitar utilizar medios engañosos o fraudulentos para recolectar y realizar el tratamiento de datos personales.

08

Garantizar la seguridad de la información de los consumidores.

09

Verificar que los datos personales sean obtenidos lícitamente y que puedan ser usados para las actividades que comprende un proyecto de comercio electrónico.

10

Capacitar a su empleados para que respeten y garanticen los derechos de los titulares de los datos.

11

Evitar contactar a las personas que no quieren recibir más publicidad y suprimir sus datos cuando lo soliciten.

12

Mejorar permanentemente la atención al cliente, no solo para fortalecer la fidelización y consolidar su confianza, sino para evitar investigaciones y problemas jurídicos.



Guía sobre el tratamiento de los datos personales para fines de comercio electrónico:

<https://www.sic.gov.co/sites/default/files/files/pdf/Guia%20marketing%2C%20publicidad%20y%20tratamiento%20de%20datos%202019.pdf>



En el sitio web se debe separar la solicitud de aceptar los términos y condiciones de las autorizaciones que se piden para el tratamiento de los datos personales.

Una cosa es que el cliente acepte los términos y condiciones pactados para la venta del producto o servicio, y otra que autorice a la empresa el tratamiento de sus datos personales.

30. Recomendaciones para hacer actividades de publicidad y mercadeo cumpliendo la Ley de Protección de Datos Personales

Algunas recomendaciones para el adecuado tratamiento de los datos personales en las estrategias de mercadeo:

01

Implementar políticas y procedimientos internos sobre protección de datos personales.

02

Solicitar el cumplimiento de las políticas de tratamiento de datos personales a los terceros que contrata para realizar las campañas de mercadeo y publicidad.

03

Verificar que los datos personales fueron obtenidos lícitamente y que pueden ser utilizados para fines de mercadeo y publicidad.

04

Recolectar los datos estrictamente necesarios para los fines de mercadeo y publicidad.

05

Evitar contactar a las personas que no autorizaron el envío de publicidad y suprimir los datos de quienes lo soliciten.

06

Garantizar los derechos de los titulares de los datos.

07

Mantener activos los canales de comunicación para una debida y oportuna respuesta a las solicitudes de los titulares.

08

Emplear las estrategias de mercadeo y publicidad en días y horarios que no afecten la tranquilidad de las personas.

09

Cumplir en la práctica lo estipulado en las políticas de tratamiento de datos personales.



Guía sobre el tratamiento de datos personales para fines de mercadeo y publicidad: https://issuu.com/quioscosic/docs/guia_marketing_publicidad_y_tratamiento_de_datos_

31. Glosario

En concordancia con la normativa vigente en materia de protección de datos personales, se tendrán en cuenta las siguientes definiciones:

Archivo: conjunto de datos grabados como una sola unidad de almacenamiento que contenga los datos personales.

Autorización: consentimiento expreso e informado del titular para llevar a cabo el tratamiento de datos personales. Se obtiene al momento de la recolección del dato.

Aviso de privacidad: comunicación verbal o escrita donde el responsable le informa al titular la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a sus datos personales.

Base de datos: conjunto organizado de datos personales objetos de tratamiento.

GUÍA PRÁCTICA SOBRE PROTECCIÓN DE DATOS PERSONALES

Causahabiente: persona que ha sucedido a otra tras su fallecimiento (heredero).

Dato personal: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Dato público: son los datos que no son semiprivados, privados o sensibles como los relativos al estado civil, profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Dato privado: aquel que por su naturaleza íntima o reservada solo es relevante para el titular.

Datos sensibles: aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, por ejemplo, aquellos que revelen el origen racial o étnico, las convicciones religiosas o filosóficas; la pertenencia a sindicatos, organizaciones sociales, de derechos humanos; la orientación política; que promuevan intereses de cualquier partido político o garanticen los derechos de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Encargado del tratamiento: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros realice el tratamiento de datos personales por cuenta del responsable del tratamiento, por ejemplo, un call center al que se le entregue la información para que realice las llamadas a nombre del responsable del tratamiento de los datos personales.

Niño, niña y adolescente: se entiende por niño o niña las personas entre los 0 y los 12 años de edad, y por adolescente las personas entre 12 y 18 años acorde con el artículo 3 de la Ley 1098 de 2006.

GUÍA PRÁCTICA SOBRE PROTECCIÓN DE DATOS PERSONALES

Responsable del tratamiento: es el negocio, sea persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, recolecte y decida sobre la base de datos y/o el tratamiento de los datos.

Titular: persona natural a la que pertenecen los datos personales que serán objeto de tratamiento, por ejemplo, clientes, proveedores, contratistas, accionistas, empleados.

Tratamiento: cualquier operación o conjunto de operaciones sobre datos personales tales como la recolección, almacenamiento, uso, circulación o supresión.

Transferencia: la transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor que, a su vez, es responsable del tratamiento y se encuentra dentro o fuera del país.

Transmisión: implica la comunicación de los datos personales, dentro o fuera del territorio colombiano, para la realización de un tratamiento realizado por el encargado por cuenta del responsable.

Supresión: la acción que el titular de los datos personales solicita al responsable y/o encargado de los datos la supresión (eliminación) total o parcial de sus datos personales, en ejercicio del derecho que le asiste de libertad y finalidad frente a su información.

Las definiciones incluidas en este documento son tomadas de la normativa vigente en Colombia, la cual regula la protección de datos personales de las personas naturales frente a su tratamiento y circulación (artículo 3, Ley 1581 de 2012; artículo 3, Ley 1266 de 2008, y artículo 3, numeral 2 del Decreto 1377 de 2013, compilado en el Decreto 1074 de 2015).



**CAMARA DE COMERCIO®
DE MEDELLIN PARA ANTIOQUIA**

Tu mejor socio.

ENCUÉTRANOS



ESCÚCHANOS

cámarafm95.9®

camaramedellin.com