PROTECCIÓN DE DATOS PERSONALES

Y SU INCIDENCIA EN AMBIENTES DIGITALES

Banco Agrario de Colombia

Crecer juntos es posible

#MisDatosMeEmpoderan

Jefatura de Gobierno, Calidad y Protección de Datos

2023

CONTENIDO

Introducción

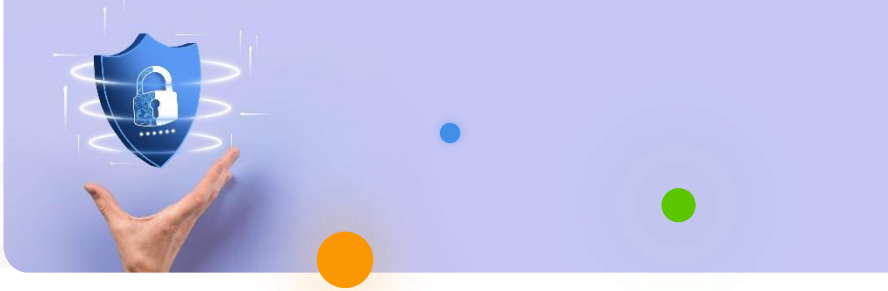
Conscientes de la trascendencia que tiene el manejo adecuado de la información, esta cartilla abordará aspectos cruciales en la protección y el tratamiento de datos personales, un tema de vital importancia en nuestro contexto actual.

Los deberes de quienes gestionamos estos datos, así como los principios que guían su manejo, son elementos clave en el pleno ejercicio del derecho al habeas data. Como miembros del Banco Agrario de Colombia, entendemos y aplicamos estos principios y deberes en nuestra labor diaria, garantizando el respeto y la protección de los derechos de los titulares de los datos.

Esta cartilla también hace énfasis en los aspectos identificados por la jurisprudencia constitucional colombiana, con proyección en su interacción normativa a las nuevas realidades sociales, entornos digitales y del consumo electrónico, donde es categórica la protección de los datos de nuestros clientes y de los demás grupos de interés.

Cristian Fernando Barrera Cerón
Jefe de Gobierno, Calidad y Protección de Datos

1 Definiciones



1.1. Titular de la Información:

Es la persona a la que pertenecen los datos personales. Es el individuo que puede ser identificado o es identificable a través de la información o datos personales que se estén tratando.

1.2. Tratamiento de Datos:

Todo proceso o conjunto de operaciones, como recopilación, almacenamiento, uso, circulación o supresión, que se realiza con datos personales. Por ejemplo, el Banco Agrario de Colombia que recopila y almacena información sobre sus clientes para procesar transacciones.

1.3. Autorización:

Es el consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

1.4. Responsable del Tratamiento:

Persona natural o jurídica, pública o privada, que por sí misma o en asociación con otros, tiene el poder de decidir sobre la base de datos y/o el tratamiento de los datos. Por ejemplo, si una tienda de ropa decide recoger datos de sus clientes para enviarles ofertas personalizadas, la tienda de ropa sería el responsable del tratamiento de esos datos.

1.5. Encargado del Tratamiento:

Es quien efectivamente maneja y procesa los datos personales, pero siempre bajo las instrucciones del responsable del tratamiento. Supongamos que la tienda de ropa contrata a una empresa de marketing para manejar su base de datos y enviar las ofertas personalizadas a los clientes. En este caso, la empresa de marketing sería el encargado del tratamiento de los datos.

2 Clasificación de los Datos y la Información

2.1 Datos Personales:

Información relacionada con una o más personas físicas identificables. Incluye cualquier dato que pueda ser utilizado para identificar, contactar o localizar a una persona. Por ejemplo, nombre completo, número de identificación o dirección de correo electrónico.

2.2. Datos Públicos:

Son aquellos cuyo conocimiento o divulgación sea de interés general porque están relacionados con la naturaleza de las actividades de las personas jurídicas o la función pública de las personas naturales. Por ejemplo, el nombre y cargo de un funcionario público o el Registro Civil de Nacimiento.

2.3. Datos Privados:

Son los datos que tienen un interés íntimo, reservado y que su conocimiento en principio solo le interesa al titular de la información. Por ejemplo, las conversaciones privadas en una plataforma de mensajería.

2.4. Datos Semiprivados:

Son aquellos que no tienen una naturaleza íntima, reservada ni pública y que debido a su naturaleza semiprivada pueden ser de interés no solo para el titular sino también para terceros. Por ejemplo, el historial crediticio.

2.5. Datos Sensibles:

Aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, como aquellos que revelan el origen racial o étnico, la orientación sexual, la salud, las convicciones religiosas y políticas.

2.6. Información Pública Clasificada:

Información privada o semiprivada de una persona física o jurídica cuyo acceso es clasificado porque puede violar derechos como la intimidad, la salud, los secretos comerciales, entre otros.

2.7. Información Pública Reservada:

Información cuya divulgación está legalmente prohibida a terceros no autorizados, como la información de defensa y seguridad nacional.

2.8. Información Protegida por la Reserva Bancaria:

Información sobre la cual las entidades supervisadas por la Superintendencia Financiera de Colombia deben mantener la confidencialidad y discreción sobre los datos de sus clientes, como los datos de movimientos financieros.

3. Derechos de la Protección de Datos Personales

*La protección de los datos personales es **un derecho fundamental.** Como titular de datos, se tienen ciertos derechos que se pueden ejercer en cualquier momento. Aquí explicaremos cada uno de estos derechos:*

Derecho de Actualización

Tienes derecho a actualizar, modificar o rectificar tus datos en los casos en que estos no sean correctos , ya no sean veraces o se hayan modificado, sean inexactos o incompletos.

Derecho a solicitar prueba de la autorización otorgada al responsable del tratamiento.

Derecho a ser informado del uso de sus datos

Derecho a presentar quejas antes la Superintendencia de Industria y Comercio

Derecho de Acceso:

Tienes derecho a saber si tus datos están siendo procesados y para qué propósito. Por ejemplo, puedes solicitar al Banco información sobre qué datos tuyos están almacenando y para qué los están utilizando.

Derecho de Rectificación:

Si encuentras que tu información personal en los registros del Banco es incorrecta o está desactualizada, como tu dirección o número de teléfono, puedes solicitar que se corrija o se rectifique en los sistemas de información.

Derecho a la revocatoria de la autorización o supresión.

Opera cuando ya no deseas que el responsable o el encargado realice el tratamiento de tus datos o que los elimine, lo anterior sucede cuando ya no quiero que me contacten para publicidad, o cuando quiero que eliminen mis datos por carecer de legitimación

Derecho a la Limitación del Tratamiento:

Si consideras que tus datos no deberían ser procesados por algún motivo, puedes pedir que el Banco limite el uso de tus datos. Por ejemplo, si has solicitado un préstamo y ya lo has pagado, puedes pedir que el Banco limite el uso de los datos relacionados con ese préstamo.

Derecho de Oposición:

Tienes el derecho a oponerte al uso de tus datos para fines específicos, como el marketing. Por ejemplo, si el Banco te envía promociones por correo electrónico y ya no deseas recibirlas, puedes solicitar que dejen de usar tus datos para este propósito.

Derecho a la Portabilidad de los Datos:

Este derecho te permite recibir tus datos en un formato que puedas transferir fácilmente a otra institución. Por ejemplo, si decides cambiar a otro Banco, puedes pedirle al Banco X que te proporcione todos los datos que tienen sobre ti en un formato que el Banco Y pueda usar.

Recuerda, *como titular de datos, siempre tienes el control y el derecho de decidir cómo se manejan y utilizan tus datos personales.*

4 Principios de Datos Personales

Este capítulo aborda los principios esenciales de la protección de datos personales en Colombia. Los principios son reglas o pautas fundamentales que rigen la recolección, almacenamiento, uso y divulgación de datos personales, y son esenciales para garantizar el respeto a los derechos fundamentales de las personas, especialmente el derecho a la privacidad y el habeas data.

Principio de Finalidad: ***Propósito Legítimo.***
Este principio estipula que los datos personales solo deben recopilarse y utilizarse con un propósito legítimo y se le debe informar al titular de los datos.

Principio de Libertad: ***Consentimiento del Titular.***
El tratamiento de datos solo puede ejercerse con el consentimiento, previo, expreso e informado del Titular.

Principio de Legalidad: ***Cumplimiento de las Leyes.***
El tratamiento de los datos debe desarrollarse conforme con la ley y las demás disposiciones en la materia.

Principio de Seguridad: ***Protección de Datos.***
Los datos se deben tratar con las medidas técnicas o humanas necesarias para otorgar seguridad, evitando su adulteración, pérdida, uso o acceso no autorizado.

Principio de Veracidad: ***Exactitud de los Datos.***
Los datos objeto de tratamiento deben ser veraces, exactos, comprensibles, completos, no pueden ser parciales, incompletos, o que induzcan a error.

Principio de Confidencialidad: ***Respeto a la Privacidad.*** Se debe garantizar la reserva de la información, se prohíbe el acceso o comunicación de datos a terceros no autorizados.

Principio de Acceso y Circulación Restringida: ***Control del Acceso.*** El tratamiento de los datos se debe sujetar a los límites establecidos en la Ley, y solo podrá realizarse por personas autorizadas.

Principio de Transparencia: ***Claridad en el Procesamiento.*** El tratamiento de datos exige que las personas tengan acceso a la información sobre cómo se procesan sus datos. Esto incluye el propósito del procesamiento, los tipos de datos y las entidades que procesan dichos datos. También tienen derecho a solicitar que se corrijan o eliminen sus datos.

Principio de Responsabilidad Demostrada:

Cumplimiento Asegurado. Las organizaciones que procesan datos personales deben demostrar que están siguiendo las leyes y regulaciones de protección de datos en su responsabilidad de garantizar que los datos se procesen de manera que se proteja la privacidad de las personas. Esto incluye tomar medidas para proteger los datos del acceso, uso o divulgación no autorizados, y para garantizar que los datos sean precisos y estén actualizados.

Principio de Protección de Datos por Defecto y Privacidad por Defecto: *: Privacidad Integrada.*

El principio de privacidad por defecto requiere que los controladores de datos configuren los sistemas de procesamiento de manera que minimicen la cantidad de datos personales recopilados, la extensión del procesamiento, el período de almacenamiento y la accesibilidad. Este principio es importante porque ayuda a garantizar que los datos personales no se recopilen, procesen o almacenen innecesariamente, lo que ayuda a proteger la privacidad de las personas.

5 Obligaciones de Quienes Tratan Datos Personales

En el contexto de la protección de datos personales, existen dos roles principales que asumen responsabilidades y obligaciones: el Responsable del Tratamiento, quien decide sobre la base de datos y/o el tratamiento de los datos, y el Encargado del Tratamiento, quien realiza el tratamiento de datos personales por cuenta del responsable. Ambos tienen un papel crucial en la protección de la privacidad y derechos de los titulares de datos personales.

6 Obligaciones Generales de los Responsables del Tratamiento

Los responsables del tratamiento tienen varias obligaciones fundamentales. Estas incluyen, pero no se limitan a:

- Obtener el consentimiento previo, expreso e informado del titular de los datos.
- Garantizar el respeto a los principios de protección de datos.
- Implementar medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad de los datos.
- Tramitar de fondo y con oportunidad los ejercicios de derechos.
- Actualizar la información cuando sea necesario y corregir cualquier error en los datos personales.

7 Obligaciones Generales de los Encargados del Tratamiento

Los encargados del tratamiento, aunque actúan bajo la dirección del responsable, también tienen responsabilidades propias, entre las cuales se incluyen:

- Realizar el tratamiento de los datos siguiendo las instrucciones del responsable.
- Cumplir la política de protección de datos del responsable y sus directrices.
- Garantizar la confidencialidad de los datos personales a los que tiene acceso.
- Implementar las medidas de seguridad necesarias.

8 Mecanismos y Autoridades para la Protección de Datos

En Colombia, la protección de datos personales goza de un marco legal sólido respaldado por garantías constitucionales. Entre estas se encuentran el derecho al hábeas data, el derecho de petición y el derecho a la tutela. Estos derechos salvaguardan la privacidad y previenen el uso inapropiado de datos personales.

Para profundizar, el hábeas data, consagrado en las leyes 1266 de 2008 y 1581 de 2012, permite a los titulares de datos el acceso, actualización, rectificación y supresión de sus datos personales. Este derecho se puede ejercer a través de dos vías legales principales: el derecho de petición y la acción de tutela, establecidos en los artículos 23 y 86 de la Constitución Nacional respectivamente.

A través del ejercicio del derecho de habeas data los ciudadanos tienen la posibilidad de solicitar información o aclaraciones sobre sus datos personales, mientras que la acción de tutela brinda un recurso judicial para proteger el derecho fundamental de habeas data cuando se ve amenazado o violado. Estas garantías constitucionales son fundamentales para mantener el respeto a la privacidad y la integridad de los datos personales en Colombia.

¿Ante qué entidades puedo presentar una queja por el tratamiento inadecuado de mis datos personales o financieros?

Existen dos autoridades de control en materia de protección de datos: la Superintendencia de Industria y Comercio en materia de datos personales, y la Superintendencia Financiera de Colombia, esta última actúa en los casos de vulneración del derecho de habeas data financiero por parte de una entidad vigilada por la mencionada autoridad, como es el caso del Banco. Las personas pueden presentar quejas ante cualquiera de las dos autoridades si creen que se le han vulnerado sus derechos de protección de datos.

Adicionalmente, los titulares de la información pueden presentar quejas ante el Defensor del Consumidor Financiero en relación con las entidades financieras, según lo dispuesto en el artículo 5º de la Ley 1328 de 2009.

¿Es posible realizar una actuación judicial para la protección de los datos?

Puede presentar una demanda si cree que se han violado sus derechos de habeas data. La demanda será atendida por un Juez Civil. También puede presentar una acción de protección al consumidor financiero en el caso de que quien viole el habeas data se trate de entidades financieras.

¿Existen medidas administrativas que se puedan iniciar por vulneración de datos?

La Superintendencia de Industria y Comercio en el marco de las facultades otorgadas en los artículos 17 y 19, de las Leyes 1266 de 2008 y 1581 de 2012, respectivamente, puede conocer de las vulneraciones que por violación de tratamiento de datos personales que presenten los titulares; la Superintendencia Financiera de Colombia – SFC podrá conocer de las infracciones al habeas data financiero, respecto de sus entidades vigiladas.

¿Se pueden emprender acciones legales bajo la Ley 1273 de 2009 (Por medio de la cual se modifica el Código Penal)? En caso afirmativo, ¿cómo y ante qué autoridades se pueden presentar? En el ámbito penal por infracciones a la protección de la información, al amparo del tipo penal consagrado en el artículo 269F de la Ley 1273 de 2009, sobre la violación de los datos personales, es posible presentar denuncia penal ante la Fiscalía General de la Nación.

¿Cuáles son las autoridades colombianas que velan por la protección de los datos?

La Superintendencia de Industria y Comercio (SIC) es la principal autoridad de protección de datos Personales en Colombia. La SIC es responsable de hacer cumplir la Ley de Protección de Datos de Colombia (Ley 1581 de 2012). La SIC puede investigar denuncias de violaciones a la protección de datos y puede imponer sanciones a las entidades que violen la ley. Por otro lado, la Ley 1266 de 2008 establece como autoridad de habeas data financiero a la Superintendencia Financiera de Colombia, pero solo respecto de las entidades vigiladas por esa autoridad, ahora bien, respecto de las demás entidades la autoridad de supervisión es la Superintendencia de Industria y Comercio.

Industria y Comercio
SUPERINTENDENCIA

sfc
Superintendencia Financiera de Colombia

La Superintendencia Financiera de Colombia (SFC) es la encargada de regular el sector financiero en Colombia. La SFC tiene un papel en la protección de datos en el sector financiero y puede investigar denuncias de violaciones de la protección de datos financieros por parte de entidades financieras.

El Juez Civil es responsable de conocer de los casos civiles, incluidos los relacionados con la protección de datos.

El Juez Penal Municipal es responsable de conocer de los casos penales, incluidos los casos relacionados con la violación de datos personales.

La Procuraduría General de la Nación de forma adicional de tener a su cargo la disciplina de los servidores públicos, tiene la función de vigilar el correcto cumplimiento de las disposiciones de privacidad, protección de datos y de transparencia de los datos públicos.

9 Régimen de Protección de Datos Personales

¿Qué disposiciones específicas dispone la Constitución Política colombiana para proteger los datos personales?

En el artículo 15 de la Constitución Política de la República de Colombia se consagra la protección de los datos, como un derecho fundamental, en el cual el titular, ostenta la calidad de propietario de sus datos. Es de resaltar que la Protección de los Datos, ha tenido un gran desarrollo jurisprudencial por La Corte Constitucional Colombiana, quien desde 1992 hasta la actualidad, se ha pronunciado con más de 180 sentencias, las cuales van de la mano con los principios internacionales de la protección de datos personales, que han sido incorporados en los textos y documentos de la Organización de las Naciones Unidas y la Unión Europea.

¿Existen en Colombia marcos normativos en materia de protección de datos?

Colombia cuenta con una mixtura de normas, que regulan la materia objeto de la presente cartilla, dentro de las importantes, encontramos, la Ley 1266 de 2008 (habeas data financiero) modificada parcialmente por la ley 2157 de 2021 (Ley de borrón y cuenta nueva), sobre el habeas data financiero y comercial destinado a calcular el nivel de riesgo crediticio; la Ley 1273 de 2009, destinada a proteger a título de bien jurídico la información y los datos personales; la Ley 1581 de 2012 la cual tiene por objeto la protección de los datos personales de forma general y completa; y la Ley 1712 de 2014 sobre transparencia de la información por parte de entidades públicas y privadas con función pública.

10 Autoridades Máximas para la Vigilancia y Control de P.D.

La Superintendencia de Industria y Comercio de Colombia está constituida por la Ley 1581 de 2012 como la Autoridad Nacional de Protección de Datos Personales, la cual tiene la función principal de supervisar y garantizar que se respeten las normas de protección de datos personales. Esta autoridad tiene el deber de exigir el respeto del derecho de protección de datos personales, sus funciones también incluyen el monitoreo del cumplimiento normativo, la realización de investigaciones sobre posibles infracciones a estas normas, y la implementación de medidas necesarias para garantizar los derechos al "habeas data" y al debido tratamiento de los datos personales, esta función la lleva a cabo a través de la Delegatura para la Protección de Datos Personales, a través de la Dirección de Investigación de Protección de Datos Personales con el apoyo de dos grupos de trabajo que a continuación se relacionan.

11 Régimen Sancionatorio SIC

La Ley 1581 de 2012 brinda a la Superintendencia de Industria y Comercio la facultad de imponer sanciones, derivando esta autoridad del poder punitivo del Estado establecido en la Constitución. Este poder punitivo del Estado está destinado a responder a incumplimientos de obligaciones, deberes y mandatos que son esenciales para la buena marcha de la administración pública, el régimen sancionatorio establece qué de forma adicional a las medidas de orden administrativo, suspensión temporal del tratamiento, es posible la imposición de sanciones económicas hasta por la suma de 2000 Salarios Mínimos Mensuales Legales Vigentes – SMMLV.

12 El Tratamiento de Datos Personales en las Entidades Públicas

Es esencial que las entidades solo recojan y manejen aquellos datos personales que son necesarios para cumplir el propósito para el cual son recogidos. Deben poder describir y justificar la necesidad de recoger estos datos en cada caso.

En ciertas circunstancias, se requiere obtener la autorización del titular de los datos para su tratamiento. Sin embargo, si se recolectan datos sin autorización, la protección de esa información y los derechos de los titulares de los datos aún deben ser respetados según la Ley 1581 de 2012.

Por último, las entidades públicas no pueden recolectar datos con propósitos indeterminados. Sólo pueden tratar datos para los fines establecidos en la ley y deben definir previamente el propósito para recolectar, usar o circular la información. Estos propósitos deben estar previamente autorizados por la Constitución y la Ley.

RECOMENDACIONES:

1. Recuerda que la Ley 1581 de 2012 es aplicable a todas las entidades estatales que manejen Datos Personales. Su cumplimiento es esencial para garantizar la privacidad y protección de dichos datos.

2. La Ley 1581 de 2012 no distingue entre entidades públicas y privadas, aunque existen algunas diferencias específicas que deben considerarse:

    a. En general, no se requiere la autorización del titular del dato cuando la información es "requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial". Sin embargo, las entidades estatales deben cumplir con todas las demás disposiciones de la Ley 1581 de 2012.

    b. Las sanciones del artículo 23 de la Ley 1581 de 2012 no aplican a las entidades estatales. En caso de presunto incumplimiento, la Superintendencia de Industria y Comercio transferirá el caso a la Procuraduría General de la Nación para la investigación correspondiente.

    c. Existen algunas excepciones al alcance de la Ley 1581 de 2012. Sin embargo, estas son situaciones excepcionales y aún deben cumplir con los principios constitucionales estipulados en el artículo 4 de la Ley 1581 de 2012.

3. Las entidades estatales deben dar estricto cumplimiento de la Ley 1581 de 2012 y el Decreto 1377 de 2013, que desarrollan los instrumentos de protección de datos, como lo son la autorización y la política de protección de datos, así como el aviso de privacidad.

4. Las entidades estatales deben mantener una gestión y registro adecuados de los datos personales recogidos, asegurándose de que sean necesarios y pertinentes para la finalidad para la que son recolectados.

5. Las entidades estatales deben asegurarse de implementar medidas de privacidad desde el diseño y por defecto, con el fin de evitar vulneraciones y garantizar el correcto tratamiento de los datos desde el inicio.

6. Es crucial informar y educar a todos los empleados y partes interesadas sobre la importancia de la protección de datos y las implicaciones de la Ley 1581 de 2012.

7. Garantice siempre el pleno y efectivo ejercicio del derecho de hábeas data para el Titular de los datos. Es esencial para proteger los derechos individuales y la privacidad.

8. Solicite, reciba y conserve una copia de la autorización otorgada por el Titular de los datos, de acuerdo con las condiciones establecidas en la Ley 1581 de 2012. Esta autorización es crucial para el correcto manejo de los datos personales.

RECOMENDACIONES:

9. Mantenga la información en un ambiente seguro y controlado para evitar su alteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. La seguridad de los datos es esencial para evitar brechas y problemas de privacidad.

10. Asegúrese de que la información proporcionada al Encargado del Tratamiento sea siempre veraz, completa, exacta, actualizada, comprobable y comprensible. Un manejo preciso y actualizado de los datos garantiza su relevancia y utilidad.

11. Actualice la información de manera oportuna, comunicando al Encargado del Tratamiento todas las novedades respecto de los datos previamente suministrados, y adopte las medidas necesarias para mantener la información actualizada.

12. Rectifique la información cuando sea incorrecta y comuníquelo de inmediato al Encargado del Tratamiento. La corrección oportuna de los datos es esencial para mantener su precisión y relevancia.

13 Del Registro Nacional de Base de Datos

La Ley 1581 de 2012 establece la obligación de registrar todas las bases de datos personales ante la Superintendencia de Industria y Comercio (SIC), autoridad a cargo del Registro Nacional de Bases de Datos (RNBD). Este registro es un directorio público que da cuenta de todas las bases de datos en operación en el país.

> *Después de una serie de prórrogas sobre el registro de bases datos, a través de la Circular 003 de 2018 la SIC, estableció los obligados a llevar a cabo el RNBD, las entidades públicas, sociedades o entidades sin ánimo de lucro que tengan activos fijos totales superiores a 100.000 Unidades de Valor Tributario - UVT (Año 2020 $3.560.700.000).*

El proceso de registro implica diversas adaptaciones y modificaciones administrativas y puede incluir varias actividades. Por ejemplo, el RNBD implica la identificación de la base de datos, el registro de la cantidad de datos almacenados, las medidas de seguridad implementadas, el origen de los datos, la transferencia o transmisión de datos a nivel nacional e internacional, la cantidad de reclamos presentados por los titulares y los incidentes de seguridad.

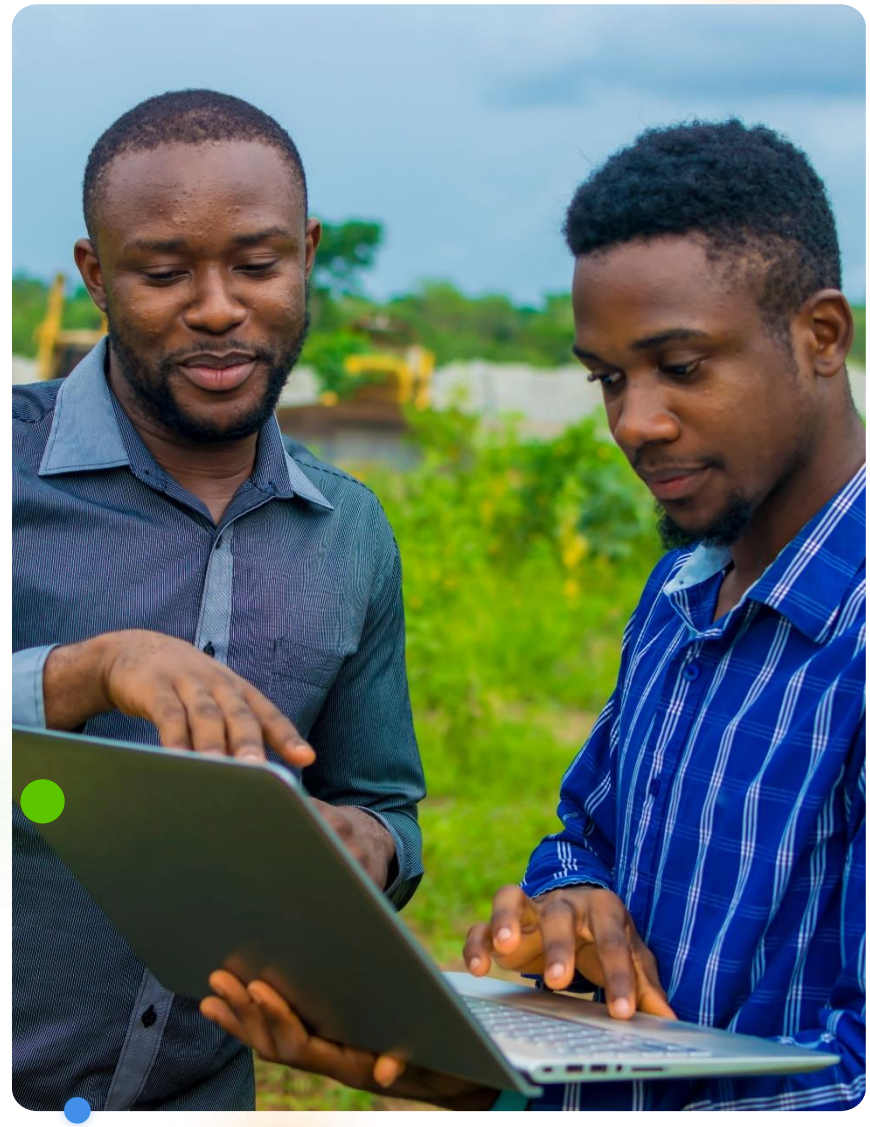
La actualización del RNBD se debe realizar en diferentes plazos: (i) dentro de los primeros diez días hábiles de cada mes cuando se realicen cambios significativos en la información registrada; (ii) anualmente, entre el 2 de enero y el 31 de marzo; (iii) dentro de los primeros quince días de febrero y agosto de cada año se deben actualizar los reclamos; (iv) las nuevas bases de datos deben ser registradas dos meses después de su creación. Este registro y actualización son requisitos clave para garantizar el manejo adecuado y seguro de los datos personales.

14 Gestión Adecuada de Datos Personales para Marketing y Publicidad

Desde el inicio, las organizaciones deben establecer cómo demostrarán su cumplimiento con las normas sobre el tratamiento de datos. Deben ser capaces de evidenciar ante la Superintendencia de Industria y Comercio que han implementado medidas apropiadas y efectivas en línea con las obligaciones establecidas en la Ley 1581 de 2012 y el Decreto 1377 de 2013, integrado en el Decreto 1074 de 2015.

Las medidas apropiadas son aquellas ajustadas a las necesidades del tratamiento de datos y las efectivas son las que permiten alcanzar los resultados deseados. Se deben adoptar acciones adecuadas, correctas, útiles, oportunas y eficientes para cumplir con los requerimientos legales para el tratamiento de datos personales.

La regulación sobre datos personales asigna responsabilidades probatorias a los encargados del tratamiento, incluyendo la conservación de evidencias de haber informado clara y expresamente al titular según lo ordena la Ley 1581 de 2012, la retención de copia de la autorización otorgada por el titular y proporcionar una descripción de los procedimientos utilizados para la recolección, almacenamiento, uso, circulación y supresión de información. Del mismo modo, existen unas recomendaciones particulares para asegurar el adecuado tratamiento de los datos, acá nuestro decálogo:



Decálogo:

1. Obtener la autorización del titular de los datos.
2. Conservar prueba de las autorizaciones otorgadas.
3. No permitir el acceso a la información por personas no autorizadas.
4. Revisar la legitimación para circular datos con terceros y autoridades.
5. Establecer las finalidades del tratamiento de los datos y comunicarlas.
6. Darle trámite a las PQR y ejercicios de derechos del habeas data.
7. Hacer un tratamiento adecuado de los datos sensibles y de menores de edad.
8. Tener un control de las bases de datos a su cargo, con seguridad y confidencialidad.
9. Establecer procedimientos que aseguren la adecuada custodia de los datos.
10. Conservar los datos por los términos legales y/o eliminarlos de forma segura.

15 Protección de Datos Personales en Ambientes Digitales

Unos de los retos de los ambientes digitales más importantes son las diversas interacciones y la amplia recolección de datos personales que en algunos casos se ha vuelto un asunto complejo por su operación o disposición, así como que los datos recabados, custodiados, almacenados y analizados generan nuevos datos que en algunos casos los consumidores desconocen de su generación o tratamiento.

De allí la importancia de pensar con cada vez más insistencia en un adecuado tratamiento de los datos, con la garantía por la privacidad y seguridad de la información, pues de forma adicional a las ventajas de cumplimiento regulatorio, se está generando un espectro de confianza que cada vez valoran más los consumidores, he incluso algunos expertos han hablado de ser una ventaja competitiva en los factores de transformación.
A continuación, te mencionamos algunas de las principales recomendaciones en materia de privacidad y protección de datos en ambientes digitales:

Protejo mis sistemas: información relacionada con una o más personas físicas identificables. Incluye cualquier dato que pueda ser utilizado para identificar, contactar o localizar a una persona. Por ejemplo, nombre completo, número de identificación o dirección de correo electrónico.

Configuro mi privacidad: es importante saber que las redes sociales presentan la posibilidad de parametrizar la privacidad, en este sentido el uso de las redes sociales debe ser de manera segura y responsable, para lo cual se debe realizar la configuración para que lo que se comparta sea visto solo por personas autorizadas por el titular.

Navego en internet de forma segura: el uso seguro de Internet, es clave para asegurar la protección de la información, pues permita a los titulares navegar protegidos con su información, por lo que se recomienda la revisión de las páginas de acceso y la instalación de herramientas que les ayude a protegerse de los riesgos cibernéticos.

Conservo mis accesos con seguridad: cuando tengo acceso sin seguridad en los diferentes entornos se facilita la actuación criminal, por eso es indispensable a protección de las cuentas, a través del uso de contraseñas seguras u otros mecanismos para evitar que personas no autorizadas accedan, y estas se deben actualizar.

Administro de forma adecuada mis cuentas: la seguridad es mucho más que disponer de usuarios y contraseñas, para la seguridad en dispositivos móviles e internet es indispensable contar con medios para su administración, que ayuden en caso de pérdida o hurto, tomar acciones como buscar, bloquear o borrar la información.

Actualizo mis sistemas: la navegación en entornos digitales demanda estar a vanguardia con los sistemas de navegación, seguridad y confidencialidad, por ello es importante la instalación de actualizaciones en programas de cómputo y aplicaciones, para reforzar su funcionalidad y para acceder a las nuevas seguridades propuestas.

Soy consciente de lo que descargo y dónde accedo: El uso de diferentes programas de cómputo y aplicaciones en entornos digitales disponen de descargas y accesos a instancias seguras para realizar transacciones, por ello me aseguro de realizar las descargas y acceder a sitios y tiendas oficiales, en el caso de ambientes transaccionales financieros, reviso que el acceso presente en la parte superior derecha en la barra de direcciones un candado cerrado, lo que significa que ese sitio web dispone de un certificado https, lo que indica que la información que envían o reciben los usuarios a través del sitio web es privada.

Soy cuidadoso con lo que publico: las publicaciones que realizas son la puerta de tu conocimiento público, por allí es posible obtener información suficiente para ser objeto de fraudes, adicionalmente tienes que ser sensible en la forma que publicas, evitando que tus interacciones generen discriminación u hostigamiento, acoso, o publicando información intima o falsa.

Sé cuál es la mejor forma de proteger mi información: Según cada entorno existen diferentes medidas de asegurar los datos de accesos intrusivos, unos de los principales en ambientes digitales es el cifrado de la información, que consiste en un conjunto de técnicas que se aplican sobre los mensajes de datos, para transformarlos en mensajes sin sentido para quien acceda sin estar autorizado para ello.

Cuento con copias de mi información: de forma adicional de que los datos cuenten con seguridad y confidencialidad, es pertinente asegurar que estos sean veraces, con calidad y que estén disponibles, es por eso que se debe contar respaldos de información como medio para garantizar que ante cualquier eventualidad se tendrá la información y los datos personales, en el momento que se necesite por parte de su titular.