ESTÁNDAR DE CUMPLIMIENTO DEL RÉGIMEN NORMATIVO DE PROTECCIÓN DE DATOS PERSONALES

PARA EL SECTOR DE CRÉDITO, COBRANZA Y BPO

COLCOB
Asociación del ecosistema crediticio y BPO

ESCUELA DE PRIVACIDAD

2025

ESTÁNDAR DE CUMPLIMIENTO DEL RÉGIMEN NORMATIVO DE PROTECCIÓN DE DATOS PERSONALES

PARA EL SECTOR DE CRÉDITO, COBRANZA Y BPO

COLCOB
Asociación del ecosistema crediticio y BPO

ESCUELA DE PRIVACIDAD

GLORIA URUEÑA
Directora Ejecutiva de COLCOB

HEIDY BALANTA
Directora Ejecutiva Escuela de Privacidad

Heidy Balanta
Directora de Escuela de Privacidad. Abogada. Magíster en Protección de Datos Personales. Magíster en Derecho Económico. Especialista en Derecho Informático y Nuevas Tecnologías. Docente de posgrados en Protección de Datos.

Cristian Fernando Barrera Cerón
Abogado. Experto en Hábeas Data Financiero. Director de Compliance | DPO | LL.M. en Derecho Procesal. Especialista en Derecho Público, Derecho Financiero y Bursátil, y Derecho Corporativo. Experto en Privacidad, Legaltech y Open Data. Docente Universitario. Conciliador

Autores Primera y Segunda Edición

Revisión Miembros **- Comité Jurídico COLCOB**

TABLA DE CONTENIDO

COLCOB
Asociación del ecosistema crediticio y BPO

ESCUELA DE PRIVACIDAD

Presentación

Dentro de los objetivos primordiales que motivaron la constitución de COLCOB estaba recopilar y consolidar las mejores prácticas que condujeran al reconocimiento del sector. Todo ello basado en sus pilares fundamentales: Profesionalización, Regulación, Consolidación y Data. Estos pilares se estructuraron alrededor de principios que, además de velar por la salud financiera de los colombianos, buscaban mantener un sano equilibrio entre las entidades de crédito y los clientes en dificultad, promoviendo el respeto mutuo.

En este contexto, y como consecuencia de lo establecido en la Ley 1266 de 2008, conocida como la Ley de Habeas Data, y la Ley 1581 de 2012, sobre el Tratamiento de Datos Personales, entre otras normativas, desde COLCOB y junto con los asociados hemos realizado un sinnúmero de actividades, talleres y conversatorios. Estas actividades han contado con la participación de distinguidos expertos en la materia, entre ellos el Superintendente de Industria y Comercio, especialistas internacionales, centrales de riesgo, consultores, oficiales de privacidad y colaboradores de empresas asociadas, quienes han compartido sus experiencias en la implementación de la regulación y la construcción de políticas organizacionales. Asimismo, hemos impulsado la sensibilización sobre la importancia de adoptar la práctica del *accountability* como un elemento clave para la mitigación de riesgos.

Estos esfuerzos han permitido alcanzar un alto nivel de cumplimiento en materia de protección de datos personales y habeas data financiero, generando confianza entre los usuarios y credibilidad ante la sociedad y las autoridades de control. Además, hemos proporcionado a la industria herramientas y buenas prácticas para proteger los datos de los titulares de información, fomentando la creatividad en su implementación y aplicación. En paralelo, hemos acompañado a los asociados y seguidores en la interpretación y adaptación a las normas, cada vez que estas han sido modificadas o ampliadas.

Por esta razón, creemos que ha llegado el momento de publicar un estándar que compile todos estos aspectos. Este estándar busca servir como una guía dinámica y de consulta general para diversos sectores, pero especialmente para nuestros asociados.

El estándar ha sido diseñado como una herramienta de apoyo para enfrentar el reto de cumplir con el régimen colombiano de protección de datos, en el marco de las disposiciones legales, tales como: Ley 1266 de 2008 sobre habeas data financiero, Ley 1273 de 2009 destinada a proteger el bien jurídico de la información y los datos personales, Ley 1581 de 2012 sobre la protección de datos personales, Ley 1712 de 2014 sobre la transparencia de la información de entidades públicas y privadas con función pública, Decreto 620 de 2020 relacionado con los servicios ciudadanos digitales y la Ley 2157 de 2021, que actualiza disposiciones sobre habeas data financiero.

Además, este estándar se constituye como un documento vivo, en constante evolución, que integra las realidades globales de protección de datos, especialmente el Reglamento General de Protección de Datos de Europa (GDPR, por sus siglas en inglés).

No es un documento estático; reconoce las nuevas realidades de la innovación, el derecho tecnológico, las Fintech y las formas emergentes de tratamiento de datos, como el *Blockchain*, los esquemas de datos abiertos y la Inteligencia Artificial. Por ello, este estándar incluye referencias para integrar el cumplimiento normativo con la explotación de nuevas tecnologías, garantizando un control adecuado del riesgo en privacidad.

Esperamos que este documento sea adoptado por la comunidad y enriquecido a través de espacios de discusión constructiva. De la mano de su autora, la doctora Heidy Balanta, directora de la Escuela de Privacidad, con los valiosos aportes de la Mesa Jurídica de la asociación y la revisión final del doctor Cristian Barrera, del Banco Agrario, hemos creado una herramienta eficaz para el cumplimiento normativo.

Finalmente, agradecemos a todos quienes hicieron posible este estándar de privacidad, por su valioso aporte a nuestras organizaciones y, en particular, al consumidor.

Gloria Urueña
Directora Ejecutiva
COLCOB

Estándares de protección de datos personales según el régimen colombiano de protección de datos

El derecho a la protección de los datos personales, reconocido como un Derecho Fundamental desde su consagración constitucional, conlleva importantes implicaciones sobre los mecanismos de salvaguarda y su relevancia en las decisiones organizacionales relacionadas con el tratamiento de información. A diferencia de otros países latinoamericanos y de las principales legislaciones internacionales en esta materia, Colombia dispone de un marco normativo diverso, múltiples instrumentos de protección y diferentes entidades encargadas de la inspección y vigilancia.

Es importante señalar que la mayoría de las organizaciones del sector crediticio, recuperación y de BPO, se encuentran bajo el ámbito de aplicación de estas normas. Esto se debe a factores como el tratamiento que realizan de la información, las finalidades de este, las categorías de datos procesados o la integración con sistemas de información públicos o privados.

En este contexto, un paso fundamental para la configuración de un programa de cumplimiento normativo en protección de datos o para el cumplimiento de los estándares de privacidad consiste en conocer la normativa aplicable, las autoridades sancionadoras y los organismos de control. A continuación, se presenta un mapa regulatorio sobre la protección de la información en Colombia.

Mapa Regulatorio de Protección de Datos – Colombia

NORMA	INSTRUMENTOS DE PROTECCIÓN	AUTORIDADES DE CONTROL
Ley 1273 de 2009: Reforma el Código Penal estableciendo el bien jurídico tutelado de la protección de la información y los datos personales	• Denuncia Penal	• Fiscalía General de la Nación • Jueces Penales
Ley 1266 de 2008 Reglamenta la protección de los datos financieros y comerciales destinados a calcular el nivel de riesgo crediticio.	Acción sancionadora ante la SIC. • Acción sancionadora ante la SFC – únicamente entidades vigiladas. • Derecho de petición. • Acción de Tutela. • Acción de protección al Consumidor financiero ante la SFC. • Proceso declarativo de protección al consumidor financiero.	• Superintendencia de Industria y Comercio – SIC. • Superintendencia Financiera de Colombia – SFC (Únicamente de las entidades vigiladas). • Jueces de la República de Colombia.

NORMA	INSTRUMENTOS DE PROTECCIÓN	AUTORIDADES DE CONTROL
Ley 1581 de 2012: Desarrolla el derecho de protección de los datos personales de forma general.	• Acción disciplinaria ante la PGN – Incumplimiento normativo. • Recurso de acceso a la información pública – Ante los jueces administrativos.	• Superintendencia de Industria y Comercio – SIC. • Procuraduría General de la Nación. • PGN (Únicamente para las autoridades públicas) .
Ley 1712 de 2014: Reglamenta la transparencia de la información y el acceso a la información pública.	• Acción disciplinaria ante la PGN • Incumplimiento normativo. • Recurso de acceso a la información pública – Ante los jueces administrativos.	• Procuraduría General de la Nación. • PGN. • Jueces administrativos.
Ley 2157 de 2021: Fortalece las obligaciones a los responsables del tratamiento en responsabilidad demostrada, y tiempos de reportes.	• Acción sancionadora ante la SIC. • Acción sancionadora ante la SFC – Únicamente entidades vigiladas. • Derecho de petición. • Acción de Tutela. • Acción de protección al consumidor financiero ante la SFC.	• Superintendencia de Industria y Comercio – SIC. • Superintendencia Financiera de Colombia – SFC (Únicamente de las entidades vigiladas).
Ley 2300 de 2023: Se establecen medidas que protegen al derecho a la intimidad de los consumidores.	• Acción sancionadora ante la SIC – Únicamente para los asuntos de protección de datos y hábeas data. • Acción sancionadora ante la SFC – Únicamente entidades vigiladas, para los asuntos de protección de datos y hábeas data. • Acción de tutela por la posible vulneración de los derechos fundamentales de intimidad o hábeas data en conexidad. • Acción de protección al consumidor financiero ante la SFC. • Proceso declarativo de protección al consumidor financiero.	• Superintendencia de Industria y Comercio – SIC. • Superintendencia Financiera de Colombia – SFC. • Jueces de la República de Colombia.

1. Estructura administrativa

La organización debe contar con una estructura administrativa proporcional a la estructura y tamaño empresarial para la adopción e implementación de políticas en tratamiento de datos personales. En este sentido, deberá establecer internamente los roles asignados para el funcionamiento de esta estructura administrativa que al final tendrá como propósito ser un Gobierno de Datos Personales articulado al Gobierno Corporativo de la organización.

Se recomienda que en dicha estructura administrativa se tengan en cuenta las siguientes instancias y/o roles:

a. Oficial de Protección de Datos o si no, un rol encargado de dar respuestas a las consultas y reclamos en materia de privacidad y protección de datos, así como del cumplimiento del régimen de protección de datos al interior de la organización. O un área que haga las veces de oficial de cumplimiento según el régimen colombiano de protección de datos.[1]
b. Oficial de Seguridad de la Información o el rol encargado de los incidentes de seguridad al interior de la organización.
c. Gestores de Datos Personales: líderes del proceso que tengan a cargo bases de datos personales o archivos con información personal.
d. Encargados del Tratamiento: Terceros con los cuales la organización tiene una relación comercial y/o contractual, y para dicha ejecución realiza el tratamiento de las bases de datos personales que administra la organización, por cuenta del responsable del tratamiento y siguiendo sus instrucciones.
e. Alta Dirección: Instancia a quien se le debe reportar el seguimiento al programa de protección de datos personales, reporte de indicadores y en general el funcionamiento del programa.

El artículo 2.2.17.5.4. del Decreto 620 de 2020 establece que para la operación de servicios ciudadanos digitales, responsable y encargado del tratamiento de datos deberá designar a una persona o área que asuma la función de protección de datos personales, quien dará trámite a las solicitudes de los Titulares para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y del capítulo 25 del Decreto 1074 de2015; y quien deberá:

1.1.1. Velar por el respeto de los derechos de los titulares de los datos personales respecto del tratamiento de datos que realice el prestador de servicios ciudadanos digitales.

1.1.2. Informar y asesorar al prestador de servicios ciudadanos digitales en relación con las obligaciones que les competen en virtud de la regulación colombiana sobre privacidad y tratamiento de datos personales.

1 La Red Iberoamericana de Protección de Datos en el año 2017 emitió los Estándares de Protección de Datos Personales, para los Estados miembros de la Red, dentro de los que se encuentra Colombia, respecto de las medidas proactivas en el tratamiento de los datos, señalando sobre las funciones del Oficial de Protección de Datos, las siguientes: "(...) a. Asesorar al responsable respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales. b. Coordinar al interior de la organización del responsable, las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia. c. Supervisar al interior de la organización del responsable el cumplimiento de la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia".

1.1.2. Supervisar el cumplimiento de lo dispuesto en la citada regulación y en las políticas de tratamiento de información del prestador de servicios ciudadanos digitales, así como del principio de responsabilidad demostrada.

1.1.4 Prestar el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos.

1.1.5 Atender los lineamientos y requerimientos que le haga la Delegatura de Protección de Datos Personales de la Superintendencia de Industria y Comercio o quien haga sus veces.

Por otro lado, la Circular Externa de 003 de 2024 la cual genera instrucciones para los administradores societarios, adoptando políticas internas efectivas para garantizar el debido Tratamiento de Datos personales en la actividad económica deben ser objeto de monitoreo y control para garantizar su cumplimiento. Para cumplir con estas instrucciones, la Guía de Responsabilidad Demostrada de la SIC, recomienda las siguientes actividades:

- Designar a una persona o área que asumirá la función de protección de datos dentro de la organización.
- Informar de manera periódica a los órganos directivos sobre la ejecución del programa de protección de datos.
- Estructurar, diseñar y administrar el programa de protección de datos.
- Establecer los controles del programa, evaluación y revisión permanente.
- Promover la elaboración e implementación de un sistema que permita administrar los riesgos del tratamiento de datos personales.
- Coordinar la definición e implementación de los controles del Programa Integral de Gestión de Datos Personales.
- Impulsar una cultura de protección de datos personales dentro de la organización.
- Mantener un inventario de las bases de datos personales en poder de la organización y clasificarlas según su tipo.
- Registrar las bases de datos de la organización en el RNBD y actualizar el reporte atendiendo a reportes de la SIC.
- Revisar los contenidos de los contratos de transmisiones internacionales de datos que se suscriban con encargados no residentes en Colombia.
- Analizar la responsabilidad de cada cargo de la organización, para diseñar un programa de entrenamiento en protección de datos personales específicos para cada uno de ellos.
- Realizar un entrenamiento general en protección de datos personales para todos los empleados de la compañía.
- Realizar el entrenamiento necesario a los nuevos empleados que tengan acceso por las condiciones de su empleo, a datos personales gestionados por la organización.

2. Identificación de actividades del tratamiento de la información personal

La organización debe documentar el ciclo de vida del tratamiento de los datos y las operaciones del tratamiento. Se debe resolver algunas preguntas: ¿cómo se recogen los datos personales?, ¿para qué se utilizan?, ¿dónde se encuentran almacenados?, ¿con quiénes circula de manera interna y de manera externa? Además, se debe verificar, identificar y plasmar:

1. Si se realizan transmisiones y/o transferencias;
2. Encargados;
3. Las finalidades del tratamiento de los datos;
4. La temporalidad de la información;
5. La supresión y disposición final de los datos.

También, se debe considerar aspectos tecnológicos asociados al tratamiento de los datos personales, algunos aspectos que se debe considerar son:

6. Sistemas de información.
7. Bases de datos.
8. Tipo de almacenamiento.
9. Medidas de seguridad actuales.

Es importante que la organización tenga claro los procesos, actividades, entradas y salidas de información personal. Asimismo, realizar un inventario de los datos personales y la clasificación de estos atendiendo a criterios de ley y enfoque de riesgos.

Para la ejecución de esta actividad es relevante que se realice teniendo en cuenta el sistema integrado de gestión de la organización, debido a que a los tratamientos de datos personales se encuentran integrados a los procesos, y deben ser vistos como parte de estos y no como casos o escenarios aislados.

La Guía de Responsabilidad Demostrada de la SIC, recomienda:

- Conocer los datos que almacenan, cómo los utilizan y si realmente los necesitan, teniendo en cuenta la finalidad para la cual los recolectan.
- Identificar en que parte del procedimiento o actividad se obtienen los datos, si deben solicitar la autorización del Titular y, de ser así, si están conservando prueba de la misma para su posterior consulta.
- En caso de manejo de datos de niños, niñas y adolescentes, implementar medidas adecuadas para garantizar la protección reforzada de dicha información.
- Asegurarse de que se esté informando al titular o a quien corresponda (datos de menores) que no existe obligación de suministrar tales datos. La clasificación de la información recopilada por la compañía, por ejemplo, en sensible, confidencial, pública, según el caso, ayuda a tener un inventario efectivo de los datos tratados por la empresa.

3. Evaluación de Riesgos en la Gestión de los Datos Personales y Evaluaciones de Impacto de Privacidad y/o Protección de Datos

La organización debe realizar una evaluación de riesgos asociados a los tratamientos de los datos personales, teniendo en cuenta el contexto, la estructura organizacional, sus procesos y procedimientos internos asociados al tratamiento de datos personales, la cantidad de bases de datos y tipos de datos personales tratados por la organización, con el propósito de 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.

A través de la Circular 002 de 2024, la Superintendencia de Industria y Comercio ha generado lineamientos para los administradores societarios. En especial, ha establecido que los administradores deben establecer los lineamientos corporativos adecuados para adoptar medidas precautorias o preventivas para proteger los derechos de los titulares de datos personales, como lo son, por ejemplo, los estudios de impacto de privacidad. Los estudios de impacto de privacidad podrían incluir, como mínimo, lo siguiente:

- Una descripción detallada de las operaciones de Tratamiento de Datos personales.
- Una evaluación de los riesgos específicos para los derechos y libertades de los Titulares de los Datos personales. En la evaluación de riesgos se espera, por lo menos, la identificación y clasificación estos.
- Las medidas previstas para evitar la materialización de los riesgos, medidas de seguridad, diseño de software, tecnologías y mecanismos que garanticen la protección de datos personales, teniendo en cuenta los derechos e intereses legítimos de los Titulares de los datos y de otras personas que puedan eventualmente resultar afectadas.

Se debe considerar que para realizar Evaluaciones de Impacto en Privacidad, la SIC ha establecido algunas actividades susceptibles de esta metodología, como son:

1. Cuando se presenten incidentes de seguridad.
2. Transferencias internacionales de datos.
3. Proyectos de inteligencia artificial.
4. Fines de marketing y publicidad.
5. Comercio electrónico.
6. Servicios de computación en la nube.
7. Actvidades de captura de información por parte de entidades del estado.

Aspectos que se deben considerar en la gestión de Riesgos, según la Guía de Responsabilidad Demostrada de la SIC:

- Identificación y manejo de riesgos asociados al tratamiento de datos personales a través de un sistema de administración de riesgos, acorde con su estructura organizacional, sus procesos y procedimientos internos asociados al tratamiento de datos personales, la cantidad de bases de datos y tipos de datos personales tratados por la empresa.
- Establecer los riesgos a que se ven expuestos los datos personales en desarrollo de su tratamiento.
- Documentar los procesos y procedimientos que se implementen dentro del ciclo de vida de los datos personales.
- Definir la metodología de identificación de riesgos asociados al tratamiento de la información personal.
- Identificar los riesgos e incidentes ocurridos, respecto de este tipo de información, en los casos que aplique.
- Medición: Tiene por objeto determinar la posibilidad de ocurrencia de los riesgos relacionados con el tratamiento de datos personales y su impacto en el caso de materializarse.
- Control: Se relaciona con las acciones que se deben tomar para controlar y/o mitigar los riesgos a que se ven expuestos los datos personales, con el fin de disminuir la posibilidad y /o las consecuencias de su materialización de estos.
- Monitoreo: Realizar un seguimiento constante para velar por las medidas que se hayan establecido sean efectivas.
- Llevar un registro de incidentes que contemple: Base de datos y datos comprometidos, titulares, fecha del incidente, y de descubrimiento, acciones correctivas realizadas y responsables.
- Se debe evaluar los riesgos periódicamente e implementar estas evaluaciones en toda la organización dentro de cada nuevo proyecto que involucre datos personales.

4. Políticas y controles para adoptar en la organización

La organización deberá adoptar los controles identificados en el plan de acción producto del ejercicio de evaluación de riesgos. No obstante, existen unos controles ya establecidos por la ley, que se deben implementar de manera obligatoria, así se encuentren o no identificados en el análisis de riesgos.

En el tratamiento de los datos personales deberán adoptarse las medidas razonables para asegurar que los datos personales que reposan en las bases de datos sean precisos y suficientes y, cuando así lo solicite el Titular o cuando el responsable haya podido advertirlo, sean actualizados, rectificados o suprimidos, de tal manera que satisfagan los propósitos del tratamiento.

La Circular Externa 003 de 2024 de la SIC, establece que los administradores societarios, deben considerar la adopción de mecanismos internos para hacer cumplir las Políticas Internas Efectivas, incluyendo herramientas de implementación, entrenamiento y programas de sensibilización, deben ser conocidas y promovidas por los administradores. Para lograr estos objetivos, se puede: i) Designar a la persona o al área que asumirá la función de protección de datos personales dentro de la organización; ii) Aprobar y verificar el real y efectivo cumplimiento de un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de las normas; iii) Establecer canales de comunicación que le permitan a la persona o al área responsable informar de manera periódica a los administradores sobre la ejecución de las Políticas Internas Efectivas de la organización.

4.1. Principios del Tratamiento de los Datos Personales

La organización deberá cumplir con los principios para el tratamiento de los datos personales en la gestión de los datos personales de las partes interesadas. En todo tiempo, deben ser observados y acatados en cualquier tipo de tratamiento de información personal.

4.2. Política de Tratamiento de Información

La organización debe contar con una Política de Tratamiento de Información que incluya como mínimo:

- Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del responsable.
- Tratamiento al cual serán sometidos los datos, esto es, recolección, usos, almacenamiento, circulación, supresión y/o disposición final de la información.

- La finalidad para la cual se recogen los datos personales.
- Derechos que le asisten como titular.
- Persona o área responsable de la atención de peticiones, consultas y reclamos ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.
- Procedimientos para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.
- Fecha de entrada en vigor de la política de tratamiento de la información y período de vigencia de la base de datos.

4.2.1. Requisitos de forma de la Política de Tratamiento de Información

Las políticas de Tratamiento de la información deberán constar en medio físico o electrónico, en un lenguaje claro y sencillo y ser puestas en conocimiento de los titulares.

4.3. Cambios en la Política

Los cambios a la política deben ser comunicados oportunamente a los titulares de los datos personales de una manera eficiente, antes de implementar las nuevas políticas. Cualquier cambio sustancial, referidos a la identificación del responsable y a la finalidad del tratamiento de los datos personales, los cuales puedan afectar el contenido de la autorización, el responsable del tratamiento debe comunicar estos cambios al titular antes de o a más tardar al momento de implementar las nuevas políticas.

4.4. Aviso de Privacidad

En los lugares de recolección de información personal, en especial, recepción, ingreso de visitantes, sala de espera, se debe adoptar un aviso de privacidad, para informarle al titular sobre la existencia de las políticas de tratamiento de información y la forma en que pueden acceder a las mismas. El aviso de privacidad deberá contener la siguiente información:

- Nombre o razón social y datos de contacto del responsable del tratamiento.
- El tratamiento al cual serán sometidos los datos y la finalidad de este.
- Los derechos que le asisten al titular.
- Los mecanismos dispuestos por el responsable para que el titular conozca la política de tratamiento de la información y sus cambios sustanciales.
- Informar al titular cómo acceder o consultar la política de tratamiento de información.
- Señalar expresamente el carácter facultativo de la respuesta a las preguntas que versen sobre datos sensibles, (siempre y cuando la organización los solicite).

4.4.1 Acreditación de la puesta a disposición del aviso de privacidad y las políticas de tratamiento de la información.

La organización debe conservar el modelo del Aviso de Privacidad ya sea en formato físico o digital, y lo puede colocar a disposición del público, en documentos, formatos electrónicos, medios verbales o cualquier otra tecnología, siempre y cuando garantice y cumpla con el deber de informar al titular.

En los casos de autenticación biométrica digital o en canales presenciales la disposición del aviso de privacidad requiere, además de las consagraciones normativas, las consagraciones sobre el adecuado tratamiento de los datos sensibles que son objeto del proceso de enrolamiento, alta del cliente o autenticación digital.

De forma adicional en los procesos de alta de los clientes en ambientes digitales, se requiere la disposición de un inventario de datos personales por actividad o producto ofertado, con la finalidad de identificar qué datos personales son necesarios para prestar sus servicios, con lo que se garantiza y cumple cabalmente con el principio de proporcionalidad, sobre el tratamiento de sólo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron. Igualmente, en los procesos de obtención de datos personales o sensibles se deben atender los deberes de seguridad y confidencialidad, implementando medidas de seguridad física, tecnológica y administrativa que permitan la circulación de los datos a través de comunicaciones seguras. Autorización del titular en los términos de la ley 1581 de 2012.

Para el tratamiento de datos personales de los titulares, se requiere la autorización previa e informada del titular. Deberá informar de manera clara y expresa lo siguiente:

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

4.4.2. Autorización del titular cuando se recojan datos personales sensibles

Además del cumplimiento de los requisitos establecidos en el punto anterior, referidos a la autorización para el tratamiento de datos, se deberá informar al titular que:

- Por tratarse de datos sensibles no está obligado a autorizar su tratamiento.
- Cuáles de los datos que serán objeto de tratamiento son sensibles y la finalidad del tratamiento, así como obtener su consentimiento expreso.

La organización debe validar que ninguna actividad que ejecute se condicione a que el titular suministre datos personales sensibles.

4.5. Mecanismos para obtener la autorización

Los responsables del tratamiento de datos personales establecerán mecanismos para obtener la autorización de los titulares o de quien se encuentre legitimado, por cualquier medio que sea legítimo conforme a las disposiciones normativas vigentes.

Estos mecanismos podrán ser predeterminados a través de medios técnicos que faciliten al titular su manifestación automatizada. Se entenderá que la autorización cumple con estos requisitos cuando se manifieste (i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización.

4.6. Conservación de la autorización

El responsable del tratamiento deberá conservar prueba del cumplimiento de lo previsto en el presente artículo y, cuando el titular lo solicite, entregarle copia de esta.

La autorización deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior, incluyendo mensajes de datos, los cuales deberán cumplir con los requisitos establecidos en la ley 527 de 1999 y demás disposiciones normativas vigentes y concordantes.

Debe asegurar de no suministrar a los operadores ningún dato cuyo suministro no esté previamente autorizado, cuando dicha autorización sea necesaria, conforme a las disposiciones en protección de datos personales.

4.7. Manual interno de políticas y procedimientos

La organización deberá contar con un Manual Interno de Políticas y Procedimientos en protección de datos personales. En dicho manual, debe incluir el procedimiento de consultas y reclamos para dar respuesta a las peticiones realizadas por los titulares de la información personal.

4.7.1. Procedimiento de consultas

- Tener un procedimiento para dar respuesta a las consultas de los titulares de la información.
- La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de esta y en todo caso dentro de los términos establecidos en las disposiciones normativas vigentes.
- 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 o los que establezcan las disposiciones normativas vigentes.
- Se deberá suministrar al titular, la información solicitada y que se encuentre 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.

4.7.2. Procedimiento de reclamos

- Tener un procedimiento de reclamos por hábeas data, esto es, 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.
- Poner a disposición del titular la información necesaria para formular el reclamo, como: 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 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.
- Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga “reclamo en trámite” y el motivo de este, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.
- 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 y en todo caso dentro de los términos establecidos en las disposiciones normativas vigentes.

- 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 o los que establezcan las disposiciones normativas vigentes.
- La información solicitada podrá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera el titular. La información deberá ser de fácil lectura, sin barreras técnicas que impidan su acceso y deberá corresponder en un todo a aquella que repose en la base de datos.

El régimen colombiano de protección de datos personales cuenta con diversas disposiciones normativas que son de especial aplicación según el tratamiento de los datos, las finalidades y la especialidad en la información, por esta razón los titulares de los datos pueden presentar diversas peticiones, quejas o reclamos, cada una de ellas en virtud de los diversos estamentos que comprenden el régi-

Legitimados para realizar el ejercicio de los derechos

Derechos	Personas legitimadas para la solicitud o el ejercer del derecho			
Hábeas Data Financiero **Ley 1266 de 2008**	Personas naturales o jurídicas titulares del dato financiero.	El representante legal del titular del dato financiero	Personas autorizadas por el titular del dato financiero.	Causahabiente* del titular del dato financiero.
Protección de Datos Personales **Ley 1581 de 2012**	Personas naturales titulares del dato personal.	El representante legal del titular del dato personal.	Personas autorizadas por el titular del dato personal	Causahabientes del titular del dato personal.
Acceso a la Información Pública **Ley 1712 De 2014**	Todas las personas naturales o jurídicas de forma directa, a través de autorización o representación.			

Plazos de respuesta al interesado o solicitante

Derecho		Plazo máximo
1.	Consulta de información financiera – Ley 1266 de 2008	10 días hábiles*
2.	Petición de información financiera – Ley 1266 de 2008	10 días hábiles*
3.	Reclamo por corrección de información financiera – Ley 1266 de 2008	15 días hábiles**
4.	Reclamo por actualización de información financier-a – Ley 1266 de 2008	15 días hábiles**
5.	Consulta de datos personales – Ley 1581 de 2012	10 días hábiles*
6.	Reclamo por corrección de datos personales – Ley 1581 de 2012	15 días hábiles**
7.	Reclamo por actualización de datos personales – Ley 1581 de 2012	15 días hábiles**
8.	Reclamo por supresión de datos personales – Ley 1581 de 2012	15 días hábiles**
9.	Petición de documentos o información pública – Ley 1712 de 2014	10 días hábiles*
10.	Solicitud de acceso a información pública – Ley 1712 de 2014	15 días hábiles**
11.	Consulta sobre información pública en razón a su cargo – Ley 1712 de 2014	30 días hábiles**
12.	Rectificación del reporte por presunta suplantación – Ley 2157 de 2021	10 días hábiles*

* Cuando no fuere posible atender la petición o consulta dentro de dicho término, se informará al interesado, antes del vencimiento del término señalado, los motivos de la demora y señalando la fecha en que se atenderá su petición o consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

** Cuando no fuere posible atender la petición dentro de dicho término, se informará al interesado, antes del vencimiento del término señalado, los motivos de la demora y señalando la fecha en que se atenderá su petición, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

*** Cuando excepcionalmente no fuere posible resolver las peticiones en los plazos señalados, el Banco debe informar esta circunstancia al interesado, antes del vencimiento del término señalado, los motivos de la demora y señalando a la vez el plazo razonable en que se resolverá o dará respuesta, que no podrá exceder del doble del inicialmente previsto.

**** Según lo dispuesto en la Ley 2157 de 2021, los casos de presunta suplantación deberán cotejarse la información sobre la suplantación en máximo 10 días hábiles, siguientes a la presentación completa de la solicitud. Es preciso aclarar que, en el caso positivo de la suplantación, la fuente de la información debe solicitar al operador de los datos la inscripción de una leyenda en el reporte de información financiera, informando que el titular fue objeto de suplantación.

En caso de que la organización no sea competente para resolver la solicitud o ejercicio de derecho de protección de datos realizado, deberá dar traslado a quien corresponda en un término máximo de dos (2) días hábiles y deberá informar de la situación al interesado o solicitante.

4.7.3. Silencio positivo

Tratándose de peticiones, quejas o reclamos que versen sobre datos financieros o el comportamiento crediticio, en virtud de lo señalado en el numeral 8 del numeral II del artículo 16 de la Ley 1266 de 2008, adicionado por el artículo 7 de la ley 2157 de 2021, este tipo de peticiones deben resolverse dentro de los términos antes señalados, so pena que, pasados estos términos, se entienda para todos los efectos legales, que la respectiva solicitud ha sido aceptada.

Es preciso mencionar que, si la organización no produce la consecuencia favorable por la respuesta emitida sin oportunidad, el peticionario puede solicitar a la Superintendencia de Industria y Comercio o a la Superintendencia Financiera de Colombia, según el caso de inspección, la imposición de las sanciones a que haya lugar conforme a la establecido en la ley 1266 de 2008 por el incumplimiento normativo.

4.8. Lineamientos comunes para ambos procedimientos

- Validar que el titular haya aportado los elementos que acrediten su identidad por los medios que la organización disponga.
- Los causahabientes del titular de la información, quienes deberán acreditar tal calidad.
- Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento conforme a las disposiciones normativas vigentes.
- Por estipulación a favor de otro o para otro.
- Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.
- Designar a una persona o área que asuma la función de protección de datos personales, que dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos.

4.9. Cumplimiento de los requisitos para reportes negativos

Uno de los instrumentos más importantes para la gestión de análisis y originación de crédito, así como para las gestiones de recuperación y cobranza es el reporte de información financiera que emiten y administran los operadores de información financiera (algunos como son: DataCredito Experian y Transunion), pues en la calidad de ***usuario***[1] o ***fuente***[2], las organizaciones reportan la información sobre el comportamiento financiero de los clientes, la cual es base principal para las actividades de análisis de riesgo de crédito.

Así las cosas, para llevar a cabo el cumplimiento de la ley 1266 de 2008 y su reciente reforma con la ley 2157 de 2021, para poder llevar a cabo el reporte negativo ante los operadores de información financiera, las organizaciones deben acreditar el cumplimiento previo de los siguientes requisitos:

1. Contar con la prueba de la contratación de la obligación, es decir con el documento vinculante que da cuenta de la existencia de la obligación, ya sea este físico o electrónico, a través de título ejecutivo, contrato de crédito o título valor.
2. Contarla autorización previa y expresa del titular del dato, con la finalidad específica de llevar a cabo el reporte negativo ante los operadores de información financiera.
3. Contar con la(s) comunicación(es) previa(s) al deudor, según lo establecido en los artículos 12 y 13 de la ley 1266 de 2008. La(s) comunicación(nes) debe(n) ser dirigida(s) a los lugares físicos o electrónicos relacionados por el cliente en dificultad, y debe ser positiva su entrega. Es importante tener en cuenta que el reporte negativo se debe realizar pasados 20 días calendario siguientes a la fecha de envío de la comunicación, o de la segunda comunicación para el caso de las obligaciones inferiores o iguales al quince por ciento (15 %) de un (1) salario mínimo legal mensual vigente.

En aquellos eventos en que los equipos de cómputo permitan el envío o recepción de correo electrónico, mensajería instantánea, o cualquier otro servicio que permita el intercambio de información, se deben contar con un sistema de registro de la información enviada y recibida, y conservar dichos registros por un periodo mínimo de 6 meses.

En el caso en que la información respectiva sea objeto o soporte de una reclamación, queja o forme parte de un proceso judicial o una actuación extrajudicial, se deberá conservar hasta el momento en que la reclamación o queja se resuelva, o el proceso o actuación finalice.

---

1 Según el artículo 3° de la Ley 1266 de 2008, se define como usuario: "(...) Usuario. El usuario es la persona natural o jurídica que, en los términos y circunstancias previstos en la presente ley, puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información".

2 Según el artículo 3° de la Ley 1266 de 2008, se define como fuente: "(...) Fuente de información. Es la persona, entidad u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, debido a autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final".

4.10. Medidas de seguridad

- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Contar con una política de seguridad de la información que incluya medidas específicas para la protección de los datos personales.

4.11. Incidentes de seguridad

Los responsables y encargados deben informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.

También, deben contar con un protocolo de respuesta en el manejo de incidentes de seguridad, conforme a la Guía para la Gestión de Incidentes de Seguridad en el Tratamiento de Datos Personales de la Superintendencia de Industria y Comercio.

- Gestión de riesgos internos y externos, que le permitan identificar sus vulnerabilidades a tiempo, se debe contar con una persona o área responsable de manejar los incidentes o vulneraciones a los sistemas de información o a los archivos físicos.
- Mecanismos para rendir informes internos y reportar los incidentes a los titulares y a la SIC. Se debe implementar mecanismos que les permitan comunicarse de manera eficiente con los titulares afectados, sobre el incidente de seguridad relacionada con sus datos personales y las posibles consecuencias, y proporcionar herramientas a dichos titulares afectados para minimizar el daño potencial o causado.
- Se debe informar como mínimo, el tipo de incidente, la fecha en que ocurrió, y la fecha en la que se tuvo conocimiento de este, la causal, el tipo de datos personales comprometidos y la cantidad de titulares afectados.

NOTA: Considerar la Guía de Gestión de Incidentes de Seguridad de la Superintendencia de Industria y Comercio para efectos de adecuar a los procedimientos internos.

4.12. Transmisiones de datos personales

La organización deberá suscribir contrato de transmisión de datos con los encargados para el tratamiento de datos personales bajo su control y responsabilidad, el cual deberá ajustarse a las disposiciones normativas vigentes y adicional señalará:

1. Los alcances del tratamiento.
2. Las actividades que el encargado realizará por cuenta del responsable para el tra-

tamiento de los datos personales.
3. Las obligaciones del encargado para con el titular y el responsable.
4. El compromiso del encargado de dar aplicación a las obligaciones de la organización, bajo la política de tratamiento de la información fijada por este y a realizar el tratamiento de datos de acuerdo con la finalidad que los titulares hayan autorizado y con las leyes aplicables.
5. Dar tratamiento, a nombre del responsable, a los datos personales conforme a los principios que los tutelan.
6. Salvaguardar la seguridad de las bases de datos en los que se contengan datos personales.
7. Guardar confidencialidad respecto del tratamiento de los datos personales.

4.12.1 Encargados del tratamiento

Cuando se entregue a un tercero el tratamiento de los datos personales de la organización, se deberá formalizar a través de un contrato de transmisión de datos personales u otro mecanismo que sea legalmente válido. El responsable deberá para con el encargado, hacerle cumplir las siguientes obligaciones:

- Los responsables del tratamiento deberán desarrollar sus políticas para el tratamiento de los datos personales y velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas.
- Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
- Realizar oportunamente la actualización, rectificación o supresión de los datos conforme a los términos de las disposiciones normativas vigentes.
- Actualizar la información reportada por los responsables del tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo;
- Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la ley; conforme al procedimiento que le ha señalado el responsable;
- Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares;
- Registrar en la base de datos la leyenda “reclamo en trámite” en la forma en que se regula en la ley;
- Insertar en la base de datos la leyenda “información en discusión judicial” una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal;
- Abstenerse de circular información que esté siendo controvertida por el titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio;
- Permitir el acceso a la información únicamente a las personas que pueden tener

acceso a ella;
- Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares;
- Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

4.12.2 Deberes que la organización tiene con el encargado

- Garantizar que la información que se suministre al encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible;
- Actualizar la información, comunicando de forma oportuna al encargado del tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada;
- Rectificar la información cuando sea incorrecta y comunicar lo pertinente al encargado del tratamiento;
- Suministrar al encargado del tratamiento, según el caso, únicamente datos cuyo tratamiento esté previamente autorizado de conformidad con lo previsto en la ley;
- Exigir al encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular;
- Informar al encargado del tratamiento cuando determinada información se encuentra en discusión por parte del titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.

Aspectos para considerar dentro del procedimiento:

1. Antes de la contratación, el proceso de contratación y compras o el proceso responsable, deberá validar con el proceso jurídico y de seguridad de la información, si el nuevo proveedor cuenta con las condiciones de seguridad de la información y de protección de datos para la contratación.
2. Elaborar contratos de transmisión de datos personales con todos los encargados del tratamiento.
3. Realizar auditorías y/o evaluaciones de cumplimiento periódicas con los encargados del tratamiento que la organización haya considerado críticos.

4.12.3 Contratos con empresas de cobranza, contact center o call center

Siendo los contratos, acuerdos y alianzas entre organizaciones originadores de crédito y las entidades externas de los servicios de recuperación de cartera y/o servicios BPO, se considera de vital importante que los respectivos instrumentos contractuales atiendan las disposiciones normativas y sectoriales en materia de

privacidad y protección de datos, contemplando para el efecto con lo siguiente:

a. Realizar la definición de los datos que serán objeto de tratamiento en virtud del contrato, contando con un desarrollo de los principios de tratamiento de los datos.
b. Establecer las obligaciones sobre la aplicación del régimen colombiano de protección de datos, citando de forma clara las normas aplicables.
c. Establecer y mencionar la calidad en la que las partes interactúan en el tratamiento de los datos, señalando para el efecto la calidad de responsable, encargado.
d. Detallar las medidas físicas y tecnológicas aplicables para aseguras la integridad, circulación restringida, seguridad y confidencialidad de la información.
e. Establecer los Acuerdos de Nivel de Servicio – ANS, para la atención de incidentes o brechas relacionadas con la seguridad de los datos.
f. Establecer los Acuerdos de Nivel de Servicio – ANS, para la atención de peticiones, quejas y reclamos, o requerimientos de autoridad.
g. Realizar la consagración de los canales seguros de comunicación de la información, así como los canales de comunicación entre las partes del contrato.
h. Definir los estándares de capacitación y formación de los operadores del contrato en materia de privacidad y protección de los datos.
i. Establecer la entrega, tratamiento y disposición final de los datos objeto de tratamiento, así como la custodia y archivo de la información, siendo esa física, digital o en la *nube*[3] .
j. Señalar la posibilidad o no, de poder ceder el contrato, realizar la subcontratación del servicio o el subencargo del tratamiento de los datos.
k. En el caso de contar con servicios a través de colaboradores ubicados por fuera de las instalaciones de la entidad responsable de los datos, se deben reglamentar las medidas para: (a) Preservar la confidencialidad, integridad y disponibilidad de la información.(b) Mitigar el riesgo de: i) extracción, almacenamiento o copia de la información manejada y ii) uso de dispositivos o medios de comunicación que no sean suministrados por la entidad para la prestación del servicio. (c) Impedir: i) el uso o conexión a redes distintas a las autorizadas para la prestación del servicio y ii) que se destinen los dispositivos y medios de comunicación para actividades distintas a la prestación de los servicios por este canal. (d) Fortalecer el monitoreo sobre las operaciones realizadas con productos cuya información haya sido gestionada en estas áreas.

4.13 Transferencias Internacionales de Datos Personales

Cuando se realicen transferencias internacionales de datos personales se debe realizar a países que cuenten con niveles adecuados de protección de datos personales según

3 La Superintendencia de Industria y Comercio – SIC, en su cartilla de protección de los datos personales en los servicios de computación en la nube (2018) estableció una serie de medidas a tener en cuenta en la contratación de servicios de computación en la nube, así mismo la Superintendencia Financiera de Colombia – SFC, a través de la Circular Externa 05 de 2019 realiza una serie de obligaciones sobre los requisitos de debida diligencia en la contratación de servicios de computación en la nube.

los estándares fijados por la SIC. Sin embargo, no es necesario cuando:
• Información respecto de la cual el titular haya otorgado su autorización expresa e inequívoca para la transferencia;
• Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del titular por razones de salud o higiene pública;
• Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable;
• Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad;
• Transferencias necesarias para la ejecución de un contrato entre el titular y el responsable del tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del titular;
• Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
• En caso de que no se encuentre dentro de las excepciones anteriormente mencionadas, debe solicitar a la SIC la declaración de conformidad relativa a la transferencia internacional de datos personales.

CARACTERÍSCTICAS	TRANSMISIÓN	TRANSFERENCIA
Tratamiento de Datos	El responsable determina cuál será el tratamiento de los datos personales por parte del encargado	El responsable receptor determina el tratamiento que le dará a los datos personales que le ha entregado el responsable emisor.
Formalidad	Las partes deben celebrar contrato de transmisión de datos personales	Las partes deben celebrar contrato de transferencia de datos personales·
Autorización	Si el titular ha dado la autorización para la transmisión de datos personales, no es necesario el contrato de transmisión. Se presume que el responsable debe obtener la autorización, a no ser que el encargado en virtud del contrato celebrado tenga como objeto recolectar la autorización.	Está prohibida a países que no proporcionen niveles adecuados de protección de datos, a no ser que el titular haya dado su autorización expresa

Restricciones	La ley no establece restricción alguna, no obstante, se debe tener en cuenta que para que opere se deben dar los supuestos anteriormente descritos.	No se puede realizar la transferencia sino se enmarca en las causales de excepción, o no se encuentra en la lista de países seguros, deberá solicitar la declaración de conformidad ante la Superintendencia de Industria y Comercio – SIC.

5. Reportes ante el Registro Nacional de Bases de Datos RNBD

Se deberán realizar los siguientes reportes ante el Registro Nacional de Bases de Datos:

- Reportar cualquier cambio sustancial a la información registrada, dentro de los primeros (10) diez primeros días hábiles de cada mes.
- Anualmente entre el 2 de enero y el 31 de marzo a partir del 2018, se debe actualizar la información contenida en el Registro Nacional de Bases de Datos (RNBD), cuando se presenten cambios sustanciales (los que se relacionen con la finalidad de la base de datos, el encargado del tratamiento, los canales de atención al titular, la clasificación o tipos de datos personales almacenados en cada base de datos, las medidas de seguridad de la información implementadas, la política de tratamiento de la información y la transferencia y transmisión internacional de datos personales).
- Las bases de datos que se creen se deberán inscribir dentro de los dos (2) meses siguientes contados a partir de su creación.
- Dentro de los quince (15) primeros días hábiles de los meses de febrero y agosto de cada año, a partir de su inscripción, se debe actualizar en el Registro Nacional de Bases de Datos, la información de los reclamos presentados por los titulares. El primer reporte de reclamos presentados por los titulares se deberá realizar en el segundo semestre de cada año, con la información que corresponda al primer semestre del respectivo año.
- Mínimo dos veces al año, se deberá actualizar la información contenida en el Registro Nacional de Bases de Datos (RNBD). El área encargada debe llevar el histórico de las solicitudes que hagan los titulares ya sea consultas o reclamos en materia de protección de datos.
- Reportar los incidentes presentados dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o el área encargada de atenderlos.

La Superintendencia de Industria y Comercio habilitó en el Registro Nacional de Bases de Datos, un módulo para el Oficial de Protección de Datos Personales, en el cual, se debe registrar los datos de contacto de la persona quien está asumiendo dicho rol, así como datos de tipo contractual.

6. Cumplimiento del Principio de Responsabilidad Demostrada

La organización debe acreditar la implementación de la ley 1266 de 2008 y sus decretos reglamentarios, teniendo en cuenta:

- La naturaleza jurídica, su tamaño empresarial, esto es, si se trata de una micro, pequeña, mediana o gran empresa.
- La naturaleza de los datos personales que realiza el tratamiento la organización.
- El tipo de tratamiento.
- Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares.

Se debe contar con la evidencia sobre la implementación efectiva de las medidas útiles y pertinentes para cumplir con las disposiciones legales.

6.1 Adopción de políticas internas

Se deben adoptar políticas internas, garantizando:

1. La existencia de una organización administrativa proporcional a la estructura y tamaño empresarial para la adopción e implementación de políticas consistentes con la ley 1266 de 2008 y la ley 1581 de 2012.
2. La adopción de mecanismos internos para poner en práctica las políticas incluyendo herramientas de implementación, entrenamiento y programas de educación.
3. Adopción de un proceso para la atención y respuesta de consultas y reclamos de los titulares sobre el tratamiento de sus datos personales.
4. Adoptar políticas que permitan asegurar la calidad de la información de los titulares, la comunicación previa para el reporte de la información negativa, la confidencialidad y seguridad de los datos personales.

6.2 Procedimientos internos

La organización debe adoptar procedimientos internos respecto a las obligaciones que tienen frente a los operadores de información. Estos procedimientos deben desarrollar como mínimo los siguientes lineamientos:

1. Procedimientos que permitan validar y garantizar que la información que suministre a los operadores de los bancos de datos o a los usuarios sea veraz, completa, exacta, actualizada y comprobable.
2. El reporte de forma periódica y oportuna al operador de todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.
3. Rectificación de la información cuando sea incorrecta e informar lo pertinente a los operadores.
4. Mecanismos eficaces para reportar oportunamente la información al operador.
5. Certificación semestral al operador, de que la información suministrada cuenta con la autorización de conformidad con lo previsto en la ley.
6. Otras notificaciones y comunicaciones al operador, informar al operador que determinada información se encuentra en discusión por parte de su titular, cuando se haya presentado la solicitud de rectificación o actualización de la misma, con el fin de que el operador incluya en el banco de datos una mención en ese sentido hasta que se haya finalizado dicho trámite.
7. Procedimientos para conservar evidencia de la comunicación remitida al titular informándole del reporte negativo. Antes de hacer el reporte.
8. Procedimiento para cumplir con la obligación de comunicación previa al titular de la información.

La Guía de Responsabilidad Demostrada de la SIC, recomienda:

• Las políticas deben implementar los principios que rigen el tratamiento de datos personales y estar documentadas. Igualmente, se deben documentar los procedimientos para la recolección o recopilación, el mantenimiento, uso y eliminación o disposición final de los datos personales.

• La recolección, almacenamiento, uso, circulación y supresión o disposición final de la información personal, incluyendo requisitos para obtener la autorización.

• La conservación y eliminación de la información personal.

• El uso responsable de la información, incluyendo controles de seguridad administrativos, físicos y tecnológicos.

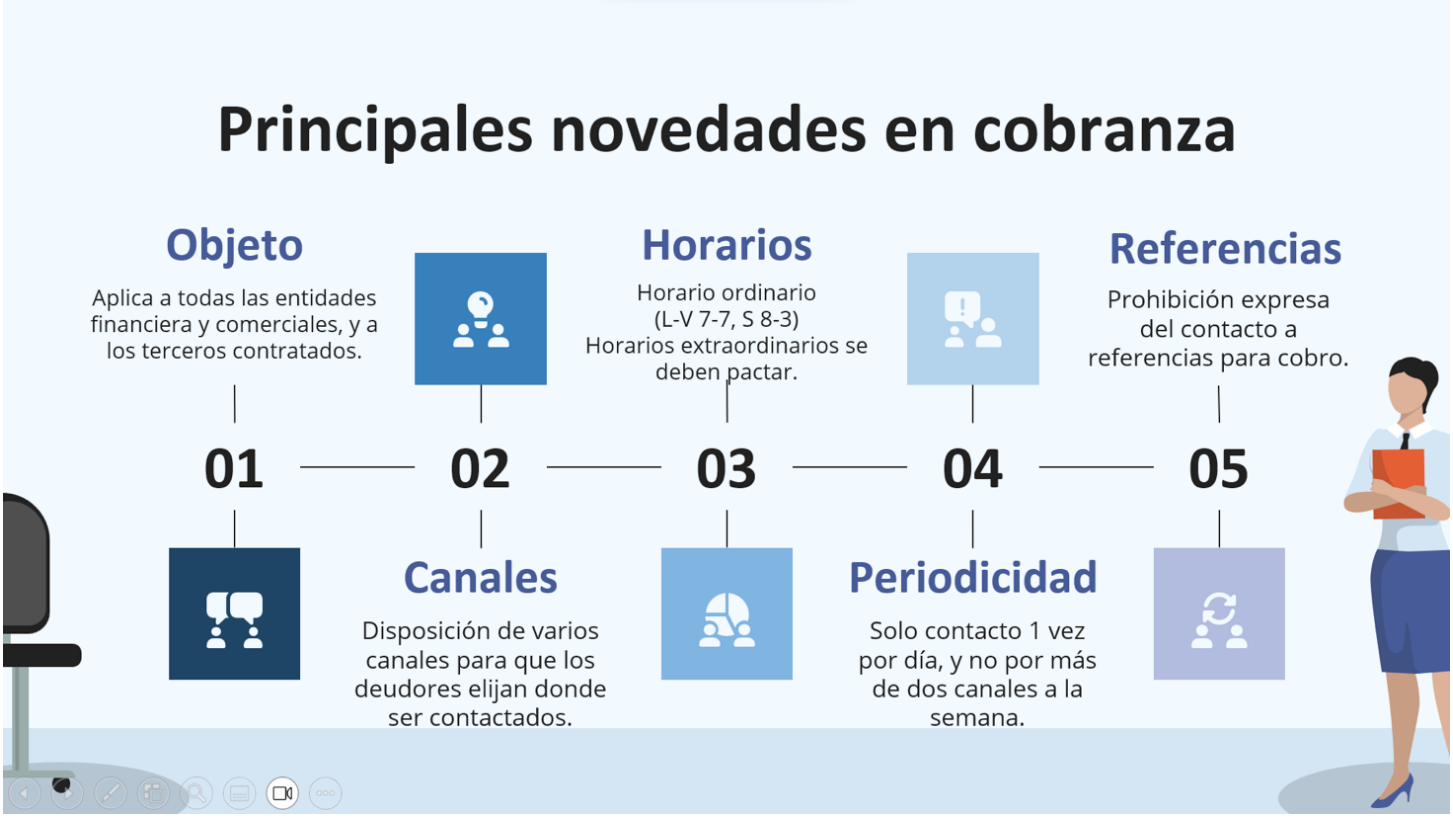
• Inclusión en todos los medios contractuales de la empresa de una cláusula de confidencialidad y de manejo de información, donde se afirme que se conoce a suficiencia la política de la empresa, se acepta, y se permite a la compañía utilizar dicha información de forma responsable.

• Procedimiento de quejas y reclamos.

• Si hay otras políticas de la organización (en talento humano, contratos, transparencia) elementos que permitan cumplir con las normas de protección de datos persona.

7. Cumplimiento de la Ley 2300 de 2023

Mediante la Ley 2300 de 2023 “por medio de la cual se establecen medidas que protejan el derecho a la intimidad de los consumidores” se dictaron normas tendientes a proteger el derecho fundamental a la intimidad de los consumidores, estableciendo los canales, el horario y la periodicidad en la que estos pueden ser contactados por las entidades vigiladas por la Superintendencia Financiera de Colombia – SFC, y todas las personas naturales y jurídicas que adelanten gestiones de cobranzas o de publicidad (marketing) de forma directa, por medio de terceros o por cesión de la obligación. Esta Ley entró en vigor el pasado 10 de octubre de 2023, y dentro de sus principales obligaciones están:



Principales novedades en cobranza

- Prohibición de cobranza en domicilio y lugar de trabajo del consumidor
- Salvedad para casos de microcréditos, crédito de fomento o agropecuario.
- Salvedad información no actualizada y accountability de contacto no positivo.
- Abstenerse de preguntar las razones de incumplimiento pero si consultar alternativas acordes a su situación financiera.

Consumidor

Autorización

Actualización

Guiones

Novedades en materia de publicidad

01 Canales

Canales autorizados para los nuevos clientes

02 Horarios

Horario ordinario (L-V 7-7, S 8-3) Horario extraordinario debe ser pactado

03 Registro

CRC desarrollo y ejecución del registro de números excluidos

Res 2229 de 2009
Res 5050 de 2016

04 Finalidad

Se debe autorizar la finalidad de envío de publicidad y leads

05 Revocación

Mecanismo ágil para revocar la autorización de envío de mensajes.

COLCOB
Asociación del ecosistema crediticio y BPO

ESCUELA DE PRIVACIDAD

7.1 Checklist de cumplimiento de la Ley 2300 de 2023

Considere este checklist como orientativo en el cumplimiento de la ley 2300 de 2023, en materia de recuperación de catera.

CHECKLIST DE CUMPLIMIENTO – LEY 2300 DE 2023				
Cumplimiento en materia de recuperación de cartera				
#	**Requerimieno**	**Cumple**		**Observacion**
		SI	**NO**	
1.	Informar y socializar previamente a los consumidores los canales de contacto a través de los cuales se puede llevar a cabo el contacto en materia de recuperación de cartera.			
2.	Poner a disposición de los consumidores de forma física o electrónica la posibilidad de elegir los canales que autoriza para su contacto.			
3.	Contactar solamente a los consumidores mediante los canales que estos autoricen.			
4.	Cuando se establezca contacto directo con el consumidor, este no podrá ser contactado para gestión de cobranza mediante varios canales dentro de esa misma semana.			
5.	Cuando se establezca contacto directo con el consumidor, este no podrá ser contactado para gestión de cobranza por más de una vez el mismo día.			
6.	Llevar a cabo el contacto para gestión de cobranza de manera respetuosa y sin afectar la intimidad personal ni familiar del consumidor.			
7.	El contacto a los consumidores para gestión de cobranza solo se puede realizar dentro del horario de lunes a viernes y de 7:00 a.m. a 7:00 p.m., y sábados de 8:00 a.m. a 3:00 p.m., excluyendo cualquier tipo de contacto con el consumidor los domingos y días festivos.			

8.	En el caso en el que el consumidor requiera el contacto para cobranza fuera del horario mencionado, deberá manifestarlo expresamente a través de un instrumento distinto al contrato o acto que rige la relación jurídica entre el consumidor y el gestor de cobranza y posterior a la suscripción de este.			
9.	Abstenerse de llevar a cabo contacto para gestiones de cobranza a las referencias personales o de otra índole.			
10.	Abstenerse de adelantar gestiones de cobranza mediante visitas al domicilio o lugar de trabajo del consumidor financiero o de servicios.			
11.	Contar con la autorización expresa del consumidor para llevar a cabo gestiones de cobranza mediante visitas al domicilio o su lugar de trabajo, en los casos de obligaciones adquiridas a través de microcréditos, crédito de fomento, desarrollo agropecuario o rural.			
12.	Contar con el registro respectivo, sobre la imposibilidad de contactar o entregar los mensajes de recuperación de cartera al consumidor, así como la desactualización de los datos en los sistemas del acreedor de la obligación.			
13.	Abstenerse de consultar al consumidor financiero el motivo del incumplimiento de la obligación.			
14.	Consultar al cliente en dificultad alternativas de pago que sean acordes con su situación financiera.			

Cumplimiento en materia de publicidad y marketing a través de mensajes cortos de texto (SMS), mensajería por aplicaciones web, correos electrónicos y llamadas telefónicas.

#	Requerimieno	Cumple		Observacion
		SI	NO	
1.	Informar y socializar previamente a los consumidores los canales de contacto a través de los cuales se puede llevar a cabo el contacto en materia de publicidad.			

2.	Poner a disposición de los consumidores de forma física o electrónica la posibilidad de elegir los canales que autoriza para su contacto.			
3.	Contactar solamente a los consumidores mediante los canales que estos autoricen.			
4.	Cuando se establezca contacto directo con el consumidor, este no podrá ser contactado para gestión de publicidad mediante varios canales dentro de esa misma semana.			
5.	Cuando se establezca contacto directo con el consumidor, este no podrá ser contactado para gestión de publicidad por más de una vez el mismo día.			
6.	El contacto a los consumidores para gestión de publicidad solo se puede realizar dentro del horario de lunes a viernes de 7:00 a.m. a 7:00 p.m., y sábados de 8:00 a.m. a 3:00 p.m., excluyendo cualquier tipo de contacto con el consumidor los domingos y días festivos.			
7.	En el caso en el que el consumidor requiera el contacto para publicidad fuera del horario mencionado, deberá manifestarlo expresamente a través de un instrumento distinto al contrato o acto que rige la relación jurídica entre el consumidor y el gestor de cobranza y posterior a la suscripción de este.			
8.	Abstenerse de obligar al consumidor a aceptar recibir mensajes comerciales de ninguna índole, cuando se realice una transacción comercial de bienes o servicios, o se ingrese a un edificio o local.			
9.	Informar al consumidor cuando lleve a cabo promociones para alimentar bases de datos.			
10	Disponer los mecanismos necesarios para que el consumidor acepte de manera explícita las promociones para alimentar bases de datos.			
11.	Habilitar y disponer de un mecanismo ágil, sencillo y eficiente para cancelar en cualquier momento la recepción de mensajes y correos, siempre y cuando no exista el deber contractual de permanecer en la respectiva base de datos de cobro.			

12.	Cumplir con las disposiciones del Registro de Números Excluidos (RNE) de la Comisión de Regulación de Comunicaciones - CRC.			

De la aplicación de la Ley 2300 de 2023 se exceptúan los contactos que tengan como finalidad informar al consumidor sobre confirmación oportuno de las operaciones monetarias realizadas, sobre ahorros voluntarios y cesantías, enviar información solicitada por el consumidor o generar alertas sobre transacciones fraudulentas, inusuales o sospechosas.

7.2 Registro de Números Excluidos - CRC

A partir de los dispuesto en el parágrafo segundo del artículo quinto de la Ley 2300 de 2023, a través de la Resolución Nro. 7356 de la Comisión de Regulación de Comunicaciones – CRC, se modificaron las disposiciones sobre el Registro de Números Excluidos – RNE, contenidas el Capítulo 1 del Título II de la Resolución CRC número 5050 de 2016, definiendo el Registro de Números Excluidos como la "(...) Base de datos en la que se podrán inscribir los consumidores y usuarios que no deseen ser contactados mediante el envío de mensajes publicitarios a través de mensajes cortos de texto (SMS), mensajería por aplicaciones o web, correos electrónicos, ni mediante llamadas telefónicas de carácter comercial o publicitario".

7.3 Concepto de contacto directo – Ley 2300 de 2023

Según lo señalado por el Consejo Asesor de la Superintendencia Financiera de Colombia – SFC, en pronunciamiento del 08 de marzo de 2024 Nro. 10115033, se concluye que, en el contexto de las actividades de cobranza a través de los diferentes medios, la expresión "contacto directo" debería entenderse como una "interacción de doble vía" entre la entidad que las realiza y el consumidor financiero receptor de las mismas.

7.4 Supervisión y vigilancia de la Ley 2300 de 2023

De acuerdo con el artículo 9° de la Ley 2300 de 2023, "el incumplimiento de las medidas de protección de que trata la presente ley, se sancionará por la Superintendencia Financiera de Colombia y la Superintendencia de Industria y Comercio, de acuerdo con el marco de competencias previsto en la Ley Estatutaria 1266 de 2008 o las normas que la modifiquen, adicionen o sustituyan".

Así las cosas, según lo dispuesto en la Circular 01 de 2024 de la Superintendencia de Industria y Comercio – SIC, y en concordancia con el artículo 17 de la Ley Estatutaria 1266 de 2008, esa superintendencia tiene a su cargo ejercer: "la función de vigilancia de los operadores, las fuentes y los usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, en cuanto se refiere a la actividad de administración de datos personales"; no obstante, cuando la fuente, usuario u

operador de información es una entidad vigilada por la Superintendencia Financiera de Colombia, esta última asume la competencia sobre la materia. Por otra parte, en lo relativo al tratamiento de datos personales, para fines de prospección comercial, según la Ley 1581 de 2012, la Superintendencia de Industria y Comercio es la autoridad llamada a realizar las funciones de inspección, vigilancia y control sobre los responsables y encargados de dicha actividad.

De este modo, se debe tener presente que la Ley 2300 de 2023, no es una norma de protección de datos, sino que complementa el régimen colombiano de protección de datos personales y de hábeas data, según las Leyes Estatutarias 1266 de 2008 y 1581 de 2012. Por lo que la vigilancia y control tanto de la Superintendencia de Industria y Comercio – SIC, como de la Superintendencia Financiera de Colombia – SFC, solo son competentes para conocer de las quejas, reclamos y denuncias que se presenten en procura de amparar el derecho fundamental de hábeas data en los siguientes asuntos:

1.	Cuando el titular manifiesta que sus datos fueron usados para adelantar gestiones de cobranza a través de un canal no autorizado, o por más de un canal.
2.	Cuando el titular manifiesta que se adelantaron gestiones de cobranza a sus referencias personales.
3.	Cuando en su calidad de referencia personal, el titular manifiesta que sus datos fueron utilizados para adelantarse gestiones de cobranza.
4.	Cuando en su calidad de avalista, codeudor o deudor solidario, el titular manifiesta que fue contactado para adelantar las gestiones de cobranza, por un canal no autorizado, o por más de un canal.
5.	Cuando el titular manifiesta que fue contactado para publicidad y marketing, por un canal no autorizado, o por más de un canal.
6.	Cuando el titular pretenda que se le suprima su información para dejar de recibir publicidad.
7.	Cuando el titular manifiesta que no ha dado autorización para recibir promociones para alimentar bases de datos.
8.	Cuando el titular manifiesta que se le está imponiendo la obligación de recibir publicidad por algún canal.
9.	Cuando el titular manifiesta que está siendo condicionado para ingresar o ser retirado de listas que le permiten acceder a bienes y servicios.

Según lo dispuesto en la Ley 2300 de 2023, los asuntos que afecten la intimidad de los consumidores solo serán del conocimiento de las superintendencias mencionadas, cuando impliquen una vulneración del derecho fundamental a la intimidad y, a su vez, afecten el derecho al hábeas data, la privacidad y la protección de datos personales.

Esto se debe a que las situaciones que no involucren una afectación a estos derechos, como aquellas que no impliquen un tratamiento indebido de datos personales, no son competencia de la SIC y la SFC, por su espectro de competencia reducido que se consagra de forma especial en las Leyes estatutarias 1266 de 2008 y 1581 de 2012. Entre estos casos se incluyen la periodicidad y horarios de contacto con los titulares, la indagación sobre el incumplimiento de obligaciones por parte del consumidor financiero, la confirmación de operaciones monetarias, ahorros voluntarios y cesantías, el envío de información solicitada por el consumidor, y las alertas sobre transacciones fraudulentas, inusuales o sospechosas.

REFERENCIAS

Comisión de Regulación de Comunicaciones. Resolución CRC 2229 de 2009.

Comisión de Regulación de Comunicaciones. Resolución CRC 5050 de 2016.

Comisión de Regulación de Comunicaciones. Resolución CRC 7356 de 2024.

Estándares de Protección de Datos Personales para los Estados Iberoamericanos 2017. Disponible en: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf.

Guía Comparativa del Reglamento General de Protección de Datos Europeo y el Régimen Colombiano de Protección de Datos Personales. Disponible en: https://escueladeprivacidad.co/wp-content/uploads/2020/05/Guia-Comparativa-Europa-Colombia.pdf.

Guía Oficial de Protección de Datos Personales. Disponible en: https://www.sic.gov.co/sites/default/files/boletin-juridico/Guia%20de%20datos%202023_0.pdf.

Guía para la aplicación del Principio de Responsabilidad Demostrada (Accountability). Disponible en: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf.

Guía para la Gestión de incidentes de seguridad en el tratamiento de datos personales. Disponible en: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia_gestion_incidentes_dic21_2020.pdf.

Guía Protección de los Datos Personales en los Servicios de Computación en la Nube (Cloud Computing). Disponible en: https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cartilla_Proteccion_datos.pdf.

Superintendencia de Industria y Comercio. Circular Externa 01 de 2024.

Superintendencia de Industria y Comercio. Circular Externa 02 de 2024.

Superintendencia de Industria y Comercio. Circular Externa 03 de 2024.

ESTÁNDAR DE CUMPLIMIENTO DEL RÉGIMEN NORMATIVO DE PROTECCIÓN DE DATOS PERSONALES

PARA EL SECTOR DE CRÉDITO, COBRANZA Y BPO

COLCOB
Asociación del ecosistema crediticio y BPO

www.colcob.com

ESCUELA DE PRIVACIDAD

www.escueladeprivacidad.co/

Contáctenos en Bogotá al 317 400 3277
www.colcob.com