ESTÁNDAR DE CUMPLIMIENTO DEL RÉGIMEN NORMATIVO DE PROTECCIÓN DE DATOS PERSONALES

PARA EL SECTOR DE CRÉDITO, COBRANZA Y BPO

colcob
ASOCIACIÓN COLOMBIANA DE LA INDUSTRIA DE LA COBRANZA

www.colcob.com

ESCUELA DE PRIVACIDAD

www.escueladeprivacidad.co

ESTÁNDAR DE CUMPLIMIENTO DEL RÉGIMEN NORMATIVO DE PROTECCIÓN DE DATOS PERSONALES

PARA EL SECTOR DE CRÉDITO, COBRANZA Y BPO

2022

Autores Primera edición

GLORIA URUEÑA
Directora Ejecutiva de Colcob

HEIDY BALANTA
Directora Ejecutiva Escuela de Privacidad

Revisión:

Cristian Barrera C.
Abogado Especialista en Protección de Datos.

Miembros Comité Jurídico Colcob

Clara Velásquez - Directora Jurídica de Refinancia
Eduardo Talero - Director Jurídico de Serlefin

TABLA DE CONTENIDO

TABLA DE CONTENIDO

Tabla de contenido interactiva
De click en cada item para ser dirigido a la página respectiva.

PRESENTACIÓN

Dentro de los objetivos primordiales que movieron a los pioneros de la constitución de Colcob, fue el de recopilar y conciliar las mejores prácticas, que condujeran al reconocimiento del sector, basados en sus pilares de profesionalización, autorregulación, data y consolidación de la industria. Todos ellos, alrededor de fundamentos que además de velar por la salud financiera de los colombianos, permitieran mantener un sano equilibrio entre las entidades de crédito y los clientes basados en el respeto de unos y otros.

Por consiguiente y como consecuencia lo establecido tanto de la Ley 1266 de 2008 de Habeas Data y de la ley 1581 de 2012, así como sus decretos reglamentarios sobre el Tratamiento de Datos Personales, entre otros, desde Colcob y de la mano de nuestros asociados realizamos un sinnúmero de actividades, talleres y conversatorios, acompañados por distinguidos expertos e instituciones en la materia, desde la Superintendencia de Industria y Comercio, expertos internacionales, centrales de riesgo, consultores, oficiales de privacidad y hasta colaboradores de empresas asociadas, compartiendo su proceso de implementación de la regulación y construcción de las políticas para sus organizaciones, hasta la sensibilización de la importancia de implementar la práctica del "accountability" como elemento clave en la mitigación del riesgo.

Esto ha permitido contar con un nivel de cumplimiento en materia de protección de datos personales y habeas data financiero, para generar confianza entre los usuarios y brindar credibilidad ante la sociedad y autoridades de control. Así mismo, proporcionando a la industria, buenas prácticas para la protección de los datos de los titulares de la información; una gran oportunidad de darle mayor creatividad a las organizaciones en su implementación y aplicación del cuidado del dato personal. En simultánea con el proceso anterior, se ha acompañado a los asociados y en general a quienes nos siguen, en la interpretación de las normas cada que se han modificado o ampliado.

Por esto hoy creemos que es el momento de publicar un estándar que recoja todos los anteriores aspectos, pero especialmente que sirva de guía y consulta dinámica, en general para los diversos sectores, pero en particular para nuestros asociados.

Un estándar diseñado como una herramienta de ayuda en el reto de cumplir con el régimen colombiano de protección de datos, al amparo de las disposiciones de la ley 1266 de 2008 sobre habeas data financiero, la ley 1273 de 2009 destinada a proteger el bien jurídico de la información y los datos personales; la ley 1581 de 2012 sobre la protección de los datos personales; la Ley 1712 de 2014 sobre transparencia de la información por parte de entidades públicas y privadas con función pública, el Decreto 620 de 2020 sobre los servicios ciudadanos digitales, y la recién ley expedida 2157 de 2021, que actualiza algunas disposiciones sobre el habeas data financiero.

Por otra parte, este estándar se constituye como una pieza sustancial de lectura y constante evolución, por la integración de las realidades de protección de datos en el mundo, especialmente del referente fundante de la privacidad en Europa, el Reglamento Europeo de la Protección de los Datos o GDPR, por sus siglas en inglés.

Así mismo, no es un documento estático que desconozca las nuevas realidades de la innovación, el derecho tecnológico, las Fintech, y las nuevas formas de tratamiento; a través del Blockchain, el Open Finance, o la Inteligencia Artificial. En este sentido, encontrará en esta pieza, algunos referentes para su integración del cumplimiento normativo y la explotación de las nuevas tecnologías, con un control adecuado del riesgo en privacidad.

Esperamos que hagan suyo este documento, que nos permitan enriquecerlo en espacios de discusión constructiva, ya que 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 con la revisión final del doctor Cristian Barrera del Banco Agrario, hemos hecho de este documento una herramienta eficaz, al momento de dar cumplimiento a la normativa.

Finalmente, a cada uno de los que hicieron posible este estándar de privacidad, gracias por este gran aporte a nuestras organizaciones en general y en particular al consumidor.

Gloria Urueña
Directora Ejecutiva
Colcob

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

La protección de los datos en Colombia y el derecho de habeas data desde su consagración constitucional es reconocido como un Derecho Fundamental con todo lo que ello implica sobre los mecanismos de protección y su relevancia en la toma de decisiones de las organizaciones que realizan tratamiento de datos, en este sentido, a diferencia de otros países latinoamericanos y principales legislaciones en materia de protección de datos, Colombia cuenta con diversas normas sobre la protección de la información, diferentes instrumentos de protección, así como diferentes entidades de inspección y vigilancia.

Al respecto, es preciso aclarar que la gran mayoría de las organizaciones del sector crediticio, de recuperaciones y BPO, se encuentran dentro del objeto de aplicación de las diversas normas de protección de datos, por el tratamiento que hacen de la información, por las finalidades del tratamiento, por las categorías de los datos objeto de tratamiento o por la integración de sistemas de información pública o privada.

En virtud de ello, uno de los principales pasos en la configuración de un compliance normativo en protección de datos o el cumplimiento de los estándares de privacidad, es conocer la normativa aplicable, las instancias sancionadoras y los organismos de control. A continuación, ponemos a disposición el mapa regulatorio de la protección de la información en Colombia.

Mapa Regulatorio de Protección de Datos – Colombia

NORMA	INSTRUMENTOS DE PROTECCIÓN	AUTORIDADES DE CONTROL
Leyes 1266 de 2008 y 2157 de 2021: Reglamentan 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.
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

NORMA	INSTRUMENTOS DE PROTECCIÓN	AUTORIDADES DE CONTROL
Ley 1581 de 2012: Desarrolla el derecho de protección de los datos personales de forma general.	• Acción sancionadora en protección de datos personales.	• 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.

Cumplimiento del Principio de Responsabilidad Demostrada

La organización debe acreditar la implementación de la ley 1266 de 2008 y la Ley 1581 de 2012, así como 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 podría 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.

Adopción de Políticas internas

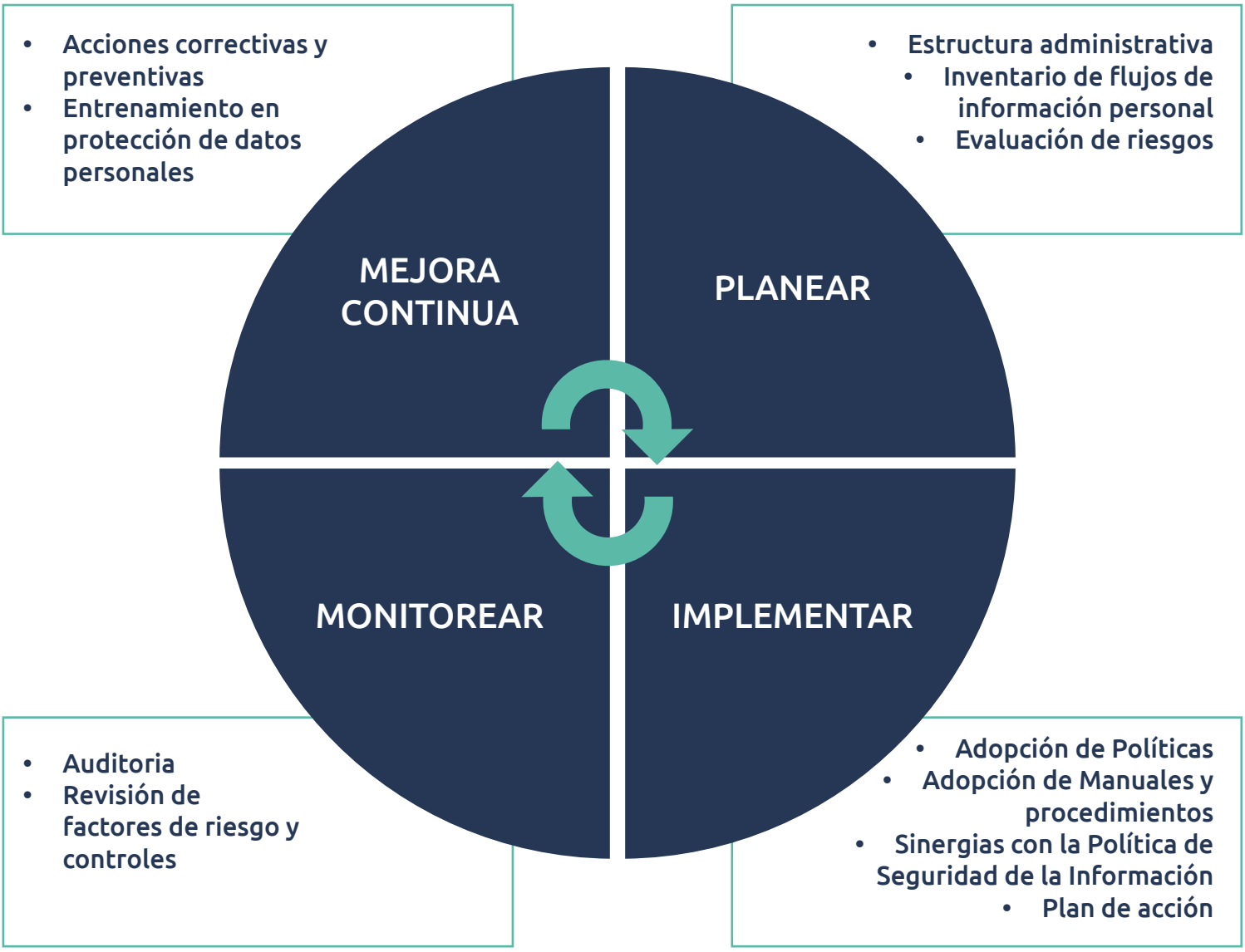
Se deben adoptar políticas internas, garantizando:

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.

NOTA: El principio de responsabilidad demostrada se encuentra desarrollado a través de la Guía de Responsabilidad Demostrada -Accountability- generada por la Superintendencia de Industria y Comercio -SIC- y es el instrumento inicial y base para el cumplimiento de este principio. Por lo que se recomienda en primera medida tener en cuenta dicho documento y posteriormente el presente estándar, el cual, esta inspirado en su desarrollo en la guía expedida por la SIC.

El presente estándar se resume en la siguiente estructura



1 PLANEAR

ESTÁNDAR DE CUMPLIMIENTO DEL RÉGIMEN NORMATIVO DE PROTECCIÓN DE DATOS PERSONALES PARA EL SECTOR DE CRÉDITO, COBRANZA Y BPO

1.1 Estructura administrativa

La organización debe contar con una estructura administrativa proporcional al 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 sino, 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).

---

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."

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.

Estos roles deben estar documentados sus responsabilidades ya sea en el manual de funciones, en los contratos de trabajo, en el instrumento que documente el Gobierno de Datos Personales roles, funciones y responsabilidades.

1.2 Inventarios de flujos de información personal

La organización en todo tiempo debe garantizar el pleno y efectivo ejercicio del derecho de hábeas data. No puede estar sobre el derecho a la protección de datos personales, ningún proceso, actividad, producto o servicio que vaya en contravía con este derecho fundamental.

En este sentido la organización debe realizar una descripción de los procedimientos usados para la recolección de los datos personales, la descripción de las finalidades para las cuales esta información es recolectada y una explicación sobre la relevancia de los datos personales en cada caso. Así mismo, deberá documentar el ciclo de vida del tratamiento de los datos, cómo se recogen, para qué se usan, dónde se encuentran almacenados, con quién se circula de manera interna y de manera externa, verificar, identificar y plasmar:

1. Si se realizan transmisiones y/o transferencias; en que países se encuentra ubicada la información
2. Quienes son los encargados.
3. Las finalidades del tratamiento de los datos.
4. La temporalidad de la información.
5. La supresión y disposición final de los datos.
6. La tecnología que se utilizar.
7. Los tipos de datos personales.

Es importante que la organización tenga claro los procesos, actividades, entradas y salidas de información personal. Así mismo, realizar un inventario de los flujos de los datos personales, de los datos personales y la clasificación de los mismos 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 deben integrar a los procesos, y deben ser vistos como parte de estos y no como casos o escenarios aislados.

1.3 Evaluación de Riesgos en la Gestión de los Datos Personales

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.

Evaluaciones de Impacto en Protección de Datos Personales

Cuando la organización tenga planeado iniciar un nuevo proyecto, producto o servicio donde involucre el tratamiento de datos personales y considere que sea probable que entrañe un alto riesgo, deberá llevar a cabo una evaluación de impacto en protección de datos, (EIPD) o evaluación de impacto en privacidad (PIA) las cuales consisten en que previo a llevar a cabo el proyecto o la novedad en el proceso interno, en la medida que la implementación comporte un alto riesgo en materia de privacidad para el individuo, ya sea por el tipo de finalidades, uso de grandes cantidades de datos, tratamiento de datos de categorías especiales o que puedan tener una afectación a los titulares de la información, que pueda entrañar un alto riesgo para los derechos fundamentales de los titulares de la información. La Evaluación de Impacto en Privacidad, deberá contemplar lo siguiente: (i) Una descripción detallada de las operaciones de tratamiento de los datos que demanda la iniciativa; (ii) Una evaluación de los riesgos específicos para los derechos y libertades de los titulares de los datos; y (iii) Las medidas y controles implementados como contención de los riesgos de la iniciativa, así como una disposición de las medidas y garantías de seguridad y la privacidad.

Se debe resaltar que las evaluaciones de impacto en protección de datos, se evalúa el riesgo para el titular, no para la organización, sin que esto, excluya, que la organización pueda evaluar y gestionar sus riesgos a través de las metodologías existentes conforme a las buenas prácticas.

2 IMPLEMENTAR

ESTÁNDAR DE CUMPLIMIENTO DEL RÉGIMEN NORMATIVO DE PROTECCIÓN DE DATOS PERSONALES PARA EL SECTOR DE CRÉDITO, COBRANZA Y BPO

2.1 Políticas y controles para adoptar en la organización

La organización deberá adoptar los controles identificados en el ejercicio de evaluación de riesgos, producto del plan de acción. Estos controles deben contar con responsables internos, fechas de cumplimiento y asignación de recursos. 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.

2.2 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.

2.3 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 vigencia de la política de tratamiento de la información y período de vigencia de la base de datos.
- Para la elaboración de la Política de Tratamiento de Información se recomienda tener como insumo el punto 2 del presente estándar, debido a que la política debe reflejar los tratamientos de los datos personales.

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.

2.4 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.

2.5 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 del mismo.
- 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).

No se debe confundir la política de tratamiento de información con el aviso de privacidad. El aviso de privacidad no suple la política, por lo que ambos instrumentos deben coexistir.

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 procesos 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.

2.6 Autorización para el tratamiento de datos personales

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 del mismo.
- 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.

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.

2.7 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.

2.8 Conservación de la autorización

El Responsable del Tratamiento deberá conservar prueba del cumplimiento de la autorización para el tratamiento de datos 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.

2.9 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.

Debido a que la ley 1581 de 2012 y la ley 1266 de 2008, establecen que se debe tener un procedimiento de consultas y reclamos, se sugiere que se contemple dentro del manual un procedimiento que integre el cumplimiento de ambas disposiciones normativas.

2.10 Procedimiento de consultas

Aspectos que la organización debe considerar en el 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 la misma 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.

2.11 Procedimiento de reclamos

Aspectos que la organización debe considerar en el procedimiento de reclamos:

- Tener un procedimiento de reclamos por habeas 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, tal 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 que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.
- Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga “reclamo en trámite” y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.
- 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.

Legitimados para realizar el ejercicio de los derechos

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 régimen de protección de datos.

Derechos	Personas legitimadas para la solicitud de información o reclamo sobre sus datos			
Habeas 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

La ley 1581 de 2012, la ley 1266 de 2008 establecen plazos similares tratándose de consultas y reclamos, en el caso de la ley 1712 de 2014 se establecen plazos mayores conforme al tipo de solicitud de información que se realiza.

	Derechos	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 financiera – Ley 1266 de 2008	15 días hábiles**

	Derechos	Plazo máximo
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***

Precisiones

* 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, se 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.

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.

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.

2.12 Lineamientos comunes para ambos procedimientos

Se debe tener en cuenta los siguientes lineamientos tratándose de consultas y reclamos:

- 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.

2.13 Cumplimiento de los requisitos para reportes negativos

Uno de los instrumentos más importantes para la gestión de análisis y origen del 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, pues en la calidad de usuario[2] o fuente[3], 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.

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

---

2 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."

3 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, en razón de autorización legal o del titular, suministra datos a un operador de información, el que a su vez los entregará al usuario final."

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. Contar con la 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 las comunicaciones previas al deudor, según lo establecido en los artículo 12 y 13 de la ley 1266 de 2008. Las comunicaciones deben ser dirigidas a los lugares físicos o electrónicos relacionados por el deudor, 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.

2.14 Procedimientos internos complementarios

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.

2.15 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 tratamiento 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.

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.

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.

2.16 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 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 que no se encuentre dentro de las excepciones anteriormente mencionadas debe solicitar la SIC la declaración de conformidad relativa a la transferencia internacional de datos personales.

Diferencias entre Transmisión y Transferencia de Datos Personales

CARACTERÍSTICA	TRANSMISIÓN	TRANSFERENCIA
Formalidad	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.

Se relacionan las principales características de la figura de Transmisión de Datos Personales y Transferencia de Datos Personales.

Contratos con empresas de cobranza, contact center o call center

Siendo los contratos, acuerdos y alianzas entre organizaciones, originadoras de crédito y las entidades externas de los servicios de recuperación de cartera y/o servicios BPO, se considera de vital importancia 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 asegurar 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 esta física, digital o en la nube[4].
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.

2.17 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 días hábiles de cada mes.
- Anualmente entre el 2 de enero y el 31 de marzo a partir del 2018, se debe actualizar la

4 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.

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.

2.18 Políticas de seguridad de la información

La Protección de Datos Personales debe articularse y complementarse con las Políticas de Seguridad de la Información. La organización debe adoptar medidas técnicas, humanas y organizacionales que eviten el deterioro, y el uso inadecuado y acceso no autorizado en el tratamiento de datos personales.

Contar con una Política de seguridad de la información no es lo mismo que contar con una Política de Tratamiento de Información, son instrumentos independientes que se complementan.

3 MONITOREAR

ESTÁNDAR DE CUMPLIMIENTO DEL RÉGIMEN NORMATIVO DE PROTECCIÓN DE DATOS PERSONALES PARA EL SECTOR DE CRÉDITO, COBRANZA Y BPO

3.1 Auditorias en Protección de Datos Personales

La evaluación y seguimiento al cumplimiento y efectividad de los controles que se han dispuesto para el cumplimiento del programa de protección de datos personales es una actividad proactiva y preventiva que permite identificar de manera temprana las desviaciones que se pueden estar presentando en la eficacia de los controles, y la identificación de nuevos escenarios de riesgos no identificados previamente, o nuevos escenarios producto de factores internos y externos.

La organización debe considerar un plan anual de autoevaluación del programa de protección de datos personales, realizando periodos previamente planeados, que tenga como propósito determinar que el programa integral de gestión de datos personales este funcionando conforme a la política de tratamiento de información, el manual interno y en general, los procedimientos establecidos para su efectivo funcionamiento, en especial, procedimientos de consultas y reclamos, de actualización, verificación y calidad de la información.

Los resultados de las auditorías deben ser reportadas a la alta dirección, con el propósito de que conozcan y tomen los correctivos producto de los hallazgos presentados, que afecten el programa de protección de datos personales, y proceder a tomar las medidas y controles que no permitan la ocurrencia o materialización de los riesgos evidenciados.

También se deben tener en cuenta la ejecución de auditorías externas, en este caso se puede solicitar a Colcob el servicio, quien lo presta a través de sus aliados.

3.2 Revisión de factores de riesgos y controles

Debido a que los programas de protección de datos personales deben ser vistos como sistemas de gestión que implican un monitoreo y continua evaluación, toda vez que no son estáticos. Esta revisión

incluye la evaluación de los factores de riesgos, teniendo en cuenta las amenazas, las vulnerabilidades, el impacto y la probabilidad de su materialización. Estos riesgos deben abordarse no solamente desde el riesgo que implica para la organización, sino para los titulares de la información.

Algunos retos que tienen las organizaciones con el monitoreo de los programas de protección de datos personales están relacionados con la variabilidad de los flujos de los datos, las tecnologías utilizadas, las personas y recursos involucrados, activos, modificaciones organizacionales y de procesos. Por lo anterior, la organización debe monitorear de manera periódica: La generación de nuevas entradas de información que se documenten a través del ciclo de vida del dato y todos los elementos que intervienen en dicho ciclo, cambios de sistema de información, tecnología, ubicación de la información, encargados del tratamiento, y en general, cualquier aspecto que modifique el tratamiento de los datos personales.

Dentro del monitoreo se debe tener en cuenta: amenazas activas internas y externas a la organización, nuevas vulnerabilidades, identificación de vulnerabilidades que se creían superadas y surgen de nuevo, cambio de impacto y probabilidad.

3.3 Gestión de vulnerabilidades e incidentes en 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.

Se recomienda tener en cuenta la Guía para la Gestión de incidentes de seguridad en el tratamiento de datos personales de la Superintendencia de Industria y Comercio.

4 MEJORA CONTINUA

ESTÁNDAR DE CUMPLIMIENTO DEL RÉGIMEN NORMATIVO DE PROTECCIÓN DE DATOS PERSONALES PARA EL SECTOR DE CRÉDITO, COBRANZA Y BPO

4.1 Adopción de medidas correctivas y preventivas

La mejora continua implica tener una visión dinámica y no estática de los programas de protección de datos personales. Una vez adoptado el programa se debe revisar, y mejorar de manera continua. En esta fase, se deben adoptar medidas proactivas y preventivas, así como medidas correctivas producto de las actividades realizadas en las fases previas del programa, ya sea producto de una auditoría, autoevaluación, planes de acción, así como fallas generadas producto de incidentes en el tratamiento de los datos personales. El propósito es la prevención de la ocurrencia.

4.2 Entrenamiento periódico

Se debe realizar entrenamientos permanentes y escalados en materia de protección de datos personales. Estos entrenamientos deben estar alineados al cumplimiento del programa de protección de datos personales. Se recomienda que los entrenamientos sean desarrollados bajo el enfoque de riesgos que debe tener la organización, complementando con la gestión adecuada de los controles que se deben adoptar durante todo el ciclo de vida de los datos personales. También se deben realizar entrenamientos según los procesos de la organización, y a la medida, teniendo en cuenta si es un proceso de servicio al cliente, de cartera, jurídico, así como entrenamiento al Oficial de protección de datos personales, o al área designada para cumplir con esta función.

Estándares de Protección de Datos Personales para los Estados Iberoamericanos 2017
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
https://escueladeprivacidad.co/wp-content/uploads/2020/05/Guia-Comparativa-Europa-Colombia.pdf

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

Guía para el tratamiento de datos personales para fines de comercio electrónico:
https://www.sic.gov.co/sites/default/files/files/pdf/Guia%20SIC%20Tratamiento%20Datos%20Personales%20ComercioElectronico(1).pdf

colcob
ASOCIACIÓN COLOMBIANA DE LA INDUSTRIA DE LA COBRANZA

www.colcob.com

ESCUELA
DE PRIVACIDAD

www.escueladeprivacidad.co

ESTÁNDAR DE CUMPLIMIENTO DEL RÉGIMEN NORMATIVO DE PROTECCIÓN DE DATOS PERSONALES

PARA EL SECTOR DE CRÉDITO, COBRANZA Y BPO

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