TABLA DE CONTENIDO

MANUAL DE POLÍTICAS DE PROTECCIÓN DE DATOS PERSONALES

1. OBJETIVO

El objetivo del presente documento denominado Manual de Políticas para la protección de datos personales, (en adelante "Manual"), es describir la forma en que se deben llevar a cabo los diferentes tratamientos que comprenden el ciclo de vida del dato personal hasta su disposición final, establecer el procedimiento que se debe llevarse a cabo cuando se presenten PQR's en esta materia, definir la forma en la que debe activarse el protocolo de incidentes de seguridad y/o violaciones a las normas de protección de datos personales y definir los reportes que deben realizarse ante el RNBD, en aras de dar cabal cumplimiento a las normas que rigen la materia, o aquellas que las complementen, sustituyan, modifiquen o deroguen.

2. ALCANCE

Este Manual es aplicable tanto a ARCILA ASOCISDOS S.A.S., en calidad de responsable del tratamiento y a sus empleadas y empleados directos e indirectos, (en adelante "operativos"), como a todas aquellas terceras personas naturales o jurídicas que realicen un tratamiento sobre datos personales de los titulares que comprenden los grupos de interés del responsable del tratamiento, por encargo de éste.

3. DEFINICIONES

Para los efectos de este Manual, se entenderá por:

- **Adolescente:** Personas entre 12 y 18 años de edad.

- **Autorización:** Consentimiento previo, expreso e informado del titular de datos personales para llevar a cabo el tratamiento de sus datos personales, la cual puede ser recolectada de manera (i) escrita, (ii) oral o (iii) mediante conductas inequívocas, que permitan concluir de manera razonable que este otorgó la autorización.

- **Aviso de privacidad:** Documento físico, electrónico o en cualquier otro formato generado por el responsable del tratamiento, que se pone a disposición del titular para el tratamiento de sus datos personales. En el aviso de privacidad se comunica al titular la información relativa a la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las características del tratamiento que se pretende dar a los datos personales.

- **Dase de datos**: Conjunto organizado de datos personales físico o electrónico (digital) que sea objeto de tratamiento manual o automatizado.

Tipo de bases de datos	
Física	**Automatizada**
Archivo físico	Digital Electrónica Medios magnéticos

- **Ciclo de vida del dato:** Etapas por las que pasan los datos personales, desde su recolección, hasta la disposición final de los mismos.

- **Datos personales**: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. la naturaleza de los datos personales puede ser pública, semiprivada, privada o sensible.

Clases de datos personales	**Ejemplos**

Datos de Identificación	Datos generales de identificación de la persona, familiares, beneficiarios o terceros. Ej: Nombre, apellido, tipo de identificación, número de identificación, fecha y lugar de expedición, nombre, estado civil, sexo, etc.
Datos específicos de Identificación	Firma, nacionalidad, datos de familia, firma electrónica, otros documentos de identificación, lugar y fecha de nacimiento o muerte, edad, etc.
Datos Biométricos	Huella, ADN, iris, Geometría facial o corporal, fotografías, videos, fórmula dactiloscópica, voz, forma de firma, etc.
Datos Morfológicos	Datos color de piel, color de iris, color y tipo de pelo, señales particulares, estatura, peso, complexión, etc.
Datos de contacto empresariales o profesionales	Dirección, teléfono, correo electrónico, etc.
Datos de contacto personales	Domicilio, teléfono, correo electrónico, etc.
Datos órdenes para procedimientos médicos	Órdenes y relación de pruebas complementarias como laboratorio, imagen, endoscópicas, patológicas, estudios, etc. NO INCLUYE RESULTADOS NI DIAGNÓSTICOS.
Datos Resultados y diagnósticos médicos	Resultados de pruebas, laboratorios, estudios, diagnósticos médicos, generales o especializados, psicológicos o psiquiátricos, medicamentos y/o tratamientos médicos o terapéuticos de cualquier tipo, etc.

Datos de Asociación	Datos relacionados con la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, religiosas, políticas
Datos sexualidad	Datos orientación sexual y preferencias sexuales
Datos de Origen	Datos de origen étnico-racial
Datos de población vulnerable	Personas de la tercera edad o menores de 18 años en condición de pobreza, personas con limitaciones sicomotoras, auditivas y visuales en condiciones de pobreza, personas víctimas de la violencia, personas en situación de desplazamiento forzado por violencia, madres gestantes o lactantes o cabeza de familia en situación de vulnerabilidad, menores en condición de abandono o protección, etc.
Datos de algún tipo de discapacidad	Personas con limitaciones sicomotoras, auditivas y visuales, etc.
Datos económicos	Datos financieros, crediticios y/o derechos de carácter económico de las personas.
Datos socioeconómicos	Estrato, propiedad de la vivienda, etc.
Datos de información tributaria	Declaración de impuestos, régimen común o simplificado, etc.
Datos patrimoniales	Bienes muebles e inmuebles, ingresos, egresos, inversiones, etc

Datos actividad económica	Actividad económica NIT
Datos laborales	Datos relacionados con la historia laboral de la persona, experiencia laboral, cargo, fechas de ingreso y retiro, anotaciones, llamados de atención, etc.
Datos educación	Datos relacionados con el nivel educativo, capacitación y/o historial académico de la persona, etc.
Datos seguridad social	EPS, IPS, ARL, fechas de ingreso/retiro EPS, AFP, etc.
Datos de acceso a Sistemas de Información	Usuarios, IP, claves, perfiles, etc.
Datos gustos y hobbies	Deportivos, ocio, gastronómicos, turismo, moda, lectura, etc.
Datos Antecedentes	Datos de antecedentes judiciales. administrativos y/o disciplinarios

- **Dato privado**: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

- **Dato público**: Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y aquel que no sea semiprivado, privado o sensible. Son públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio, a su calidad de comerciante o de servidor público y aquellos que puedan obtenerse sin reserva alguna. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales, que no estén sometidos a reserva.

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

  A los datos personales de niños, niñas y/o adolescentes, se les aplicarán las mismas normas y procedimientos que a los datos sensibles, y no se le dará tratamiento alguno que pueda vulnerar o amenazar su desarrollo físico, mental y emocional.

- **Datos semiprivados**: Son aquellos que no tienen una naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular, sino a un grupo de personas o a la sociedad en general. Se entiende por dato semiprivado, entre otros, la información relacionada con seguridad social y con el comportamiento financiero y crediticio.

- **Encargado del tratamiento**: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.

- **Fuente de información:** 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 esos datos a un operador de información, el que a su vez los entregará al usuario final.

  Para los efectos de este manual, se entenderá que la fuente es el responsable del tratamiento.

- **Inventario de bases de datos:** Documento mediante el cual se identifican las bases de datos del responsable del tratamiento y se caracterizan de acuerdo al grupo de interés, tipos de datos y finalidades para el tratamiento.

- **Ley 1266 de 2008:** Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones

- **Ley 1581 de 2012:** Ley Estatutaria por la cual se dictan disposiciones generales para la protección de datos personales diferentes a los regulados a través de la Ley 1266 de 2008.

- **Grupos de interés:** Para los efectos de este Manual, se entenderán como grupos de interés todos los grupos de personas naturales respecto de las cuales el responsable del tratamiento y/o los encargados del tratamiento realicen algún tratamiento de datos personales.

- **Niño o niña:** Personas entre los 0 y 12 años.

- **Oficial de protección de datos personales:** Persona o área responsable de velar porque se atiendan las PQR's que se presenten en materia de protección de datos personales y de velar porque se cumplan las políticas, directrices y procedimientos que conforman el Programa de protección de datos personales.

  El responsable del tratamiento, tendrá un oficial de protección de datos personales designado en la POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES (en adelante "Política de Privacidad").

- **Operativo:** Empleadas y empleados directos e indirectos, practicantes o aprendices del responsable del tratamiento que realicen algún tipo de tratamiento sobre datos personales.

- **Operador de la información:** Persona, entidad u organización que recibe de la fuente de información, datos personales comerciales, financieros o crediticios, sobre varios titulares de la información, los administra y los pone en conocimiento de los usuarios bajo los parámetros de la Ley 1266 de 2008.

- **PQR's:** Peticiones, quejas, consultas, sugerencias, reclamos y denuncias en materia de protección de datos personales.

- **Protección de datos**: Son todas las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- **Responsable de base de datos:** Operativo al que le fue designada la responsabilidad de realizar seguimiento y velar por el cumplimiento del programa de datos personales dentro del área respecto de la cual ostenta la calidad de responsable de base de datos y reportar al oficial de protección de datos personales las actualizaciones a las mismas o la

ocurrencia de incidentes de seguridad o violaciones sobre datos que reposen en estas bases de datos.

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

- **Responsable del tratamiento receptor:** Responsable del tratamiento que recibe datos personales de otro responsable del tratamiento (responsable del tratamiento remitente) para que realice tratamiento a los mismos por cuenta propia, bien sea directamente, o a través de terceros encargados del tratamiento.

- **Responsable del tratamiento remitente:** Responsable del tratamiento que transfiere datos personales contenidos en sus bases de datos a otro responsable del tratamiento (responsable del tratamiento receptor), para que éste último decida sobre los mismos y realice tratamiento por cuenta propia, bien sea directamente, o a través de terceros encargados del tratamiento.

- **Tabla de retención documental:** Se define como el listado de series, con sus correspondientes tipos documentales, a las cuales se asigna el tiempo de permanencia en cada etapa del ciclo de vida de los documentos e información que contenga datos personales. Es el instrumento que permite establecer cuáles son los documentos e información del responsable del tratamiento su necesidad e importancia en términos de tiempo de conservación y preservación y qué debe hacerse con ellos una vez finalice su vigencia o utilidad**.**

- **Titular:** Para los efectos de la Ley 1266 de 2008, es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías consagrados en dicha Ley y las normas que la complementen, modifiquen, sustituyan o deroguen. Para los efectos de la Ley 1581 de 2012, es la persona natural cuyos datos personales sean objeto de tratamiento.

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

- **Transmisión:** Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia

cuando tenga por objeto la realización de un Tratamiento por el encargado del tratamiento por cuenta del responsable del tratamiento.

- **Tratamiento**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, actualización, uso, circulación, transferencia, transmisión o supresión.

- **Valoración documental:** Proceso técnico intelectual que consiste en analizar la producción documental y de información del responsable del tratamiento y/o encargado del tratamiento de datos personales con el fin de determinar aquellos que tienen un valor inmediato o primario y los que poseen un valor mediato o secundario.

Los términos y definiciones se extraen de las normas y se entiende que incluyen en su referencia, cuando aplique, a hombres y mujeres sin distinción de sexo o identidad de género.

4. PROTOCOLO PARA EL TRATAMIENTO DE DATOS PERSONALES

Para realizar cualquier tratamiento, el responsable del tratamiento, los operativos y los encargados del tratamiento, deberán seguir los pasos específicos que se definen a continuación, para cada ciclo de vida del dato personal.

4.1. RECOLECCIÓN

Para la recolección de datos personales, sin importar cuál sea la técnica a utilizar, se deberán seguir los siguientes pasos:

4.1.1. Identificar el Grupo de Interés

Se debe identificar el grupo de interés al cual pertenecen los titulares cuyos datos personales serán recolectados y validar si ya existe una base de datos creada para estos, dentro del inventario de bases de datos. En caso de no estar creada, deberá informarlo al Oficial de protección de datos personales, para que éste último procesa a incluirla.

4.1.2. Identificar las Finalidades para las cuales se requiere recolectar Datos Personales:

Las finalidades para las cuales se van a recolectar los datos personales deben ser claras, proporcionales, pertinentes y adecuadas, y se debe verificar que éstas se encuentren incluidas dentro de la Política de privacidad.

En caso de no estar incluidas las finalidades o alguna(s) de ellas dentro de la Política de Privacidad, el operativo deberá directamente, o a través del responsable de base de datos de su área o proceso, reportarlo al oficial de protección de datos personales, antes de realizar el proceso de recolección de datos personales, con el fin de que este último, realice las gestiones pertinentes para la inclusión de las mismas en la Política de Privacidad y proceda con su divulgación.

4.1.3. Identificar los Datos Personales que se van a recolectar para cumplir con las Finalidades previamente identificadas y la naturaleza de los mismos:

El operativo debe identificar qué datos personales se van a recolectar e identificar su naturaleza:

Datos Personales	**Naturaleza del Dato**
Datos de Identificación	Público
Datos de contacto empresariales o profesionales	Público
Datos actividad económica	Público
Datos específicos de Identificación	Semiprivado
Datos económicos	Semiprivado
Datos de información tributaria	Semiprivado
Datos patrimoniales	Semiprivado
Datos laborales	Semiprivado
Datos educación	Semiprivado
Datos seguridad social	Semiprivado
Datos Antecedentes	Privado

Datos de contacto personales	Privado
Datos órdenes para procedimientos médicos	Privado
Datos socioeconómicos	Privado
Datos de acceso a Sistemas de Información	Privado
Datos gustos y hobbies	Privado
Datos morfológicos	Privado
Datos Biométricos	Sensible
Datos órdenes para procedimientos médicos	Sensible
Datos resultados y diagnósticos médicos	Sensible
Datos de asociación	Sensible
Datos sexualidad	Sensible
Datos de origen	Sensible
Datos de población vulnerable	Sensible
Datos de algún tipo de discapacidad	Sensible
Datos niños, niñas y/o adolescentes	Sensible

Los datos de contacto empresariales o profesionales son de naturaleza pública, siempre y cuando se utilicen para los fines propios de la empresa o profesión. Sin embargo, adquieren el carácter de privados, cuando se utilizan para otras finalidades.

Cualquier dato personal puede ser dato sensible, si tiene la potencialidad de generar discriminación.

4.1.4. Identificar si se requiere Autorización para el Tratamiento de los Datos Personales

Se debe identificar según la naturaleza de los datos personales que se pretenden recolectar, si se requiere contar con autorización para el tratamiento de los mismos:

Naturaleza del Dato	Autorización
Público	No requiere
Semiprivado	Requiere
Privado	Requiere
Sensible	Requiere

No se podrán recolectar datos personales sin autorización del titular, salvo por las excepciones contenidas en las normas vigentes, incluyendo:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial
- Datos de naturaleza pública
- Casos de urgencia médica o sanitaria (siempre que no sea posible recolectar la autorización)
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos
- Datos relacionados con el registro civil de las personas
- Mandato legal o judicial que releve del consentimiento

Los datos personales que se encuentren en fuentes de acceso público, con independencia del medio por el cual se tenga acceso, entendiéndose por tales aquellos datos o bases de datos que se encuentren a disposición del público, pueden ser tratados por cualquier persona siempre y cuando, por su naturaleza, sean datos públicos o se esté dentro de las excepciones antes mencionadas.

4.1.5. Identificar condición de Titulares

Se debe identificar si los titulares cuyos datos personales serán recolectados, son mayores de edad, menores de edad (niños, niñas y/o adolescentes), o personas incapaces.

En caso de ser mayores de edad, la autorización para el tratamiento de datos personales, debe provenir directamente del titular, sus causahabientes, o un apoderado.

En caso de ser menores de edad, la autorización deberá provenir de sus padres o de quienes representen legalmente al menor, previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

En caso tal que el titular sea una persona incapaz, deberá otorgar la autorización el titular o su tutor, de acuerdo con lo dispuesto por las normas vigentes.

En cualquier caso, se deberá verificar la identidad de quien otorga la autorización, y requerir la acreditación de la calidad en la que actúa.

4.1.6. Verificar si se cuenta con autorización o recolectarla

En caso de requerir autorización para el tratamiento de los datos personales, previo a la recolección de los datos, el operativo deberá verificar si el responsable del tratamiento ya cuenta con la autorización del titular para dar tratamiento a los datos personales para las finalidades identificadas.

En caso de no contar con la autorización para alguna(s) de las finalidades identificadas, esta deberá solicitarse a más tardar en el momento de la recolección de los datos personales y deberá informarse al titular o a su representante, los datos personales que serán recolectados, así como todas las finalidades específicas y tratamientos para los cuales se obtiene el consentimiento. Este requisito podrá suplirse bien sea mediante un aviso de privacidad o poniendo a disposición inmediata del titular o su representante, la Política de Privacidad.

En el tratamiento de datos personales sensibles, deberán cumplirse las siguientes obligaciones:

a. Informar al titular que por tratarse de datos sensibles no está obligado a autorizar su tratamiento.
b. Informar al titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de tratamiento son sensibles y la finalidad del tratamiento, así como obtener su consentimiento expreso.

Ninguna actividad podrá condicionarse a que el titular suministre datos personales sensibles, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización, o que sea imposible desarrollar la actividad sin el tratamiento de dichos datos.

En caso de haber cambios sustanciales en el contenido de la Política de Privacidad en relación con la identificación del responsable y las finalidades del tratamiento de los datos personales, estos deberán ser comunicados al titular y se deberá obtener una nueva autorización a más tardar al momento de implementar los nuevos cambios introducidos en la Política de Privacidad.

La autorización podrá ser recolectada por escrito, de forma oral o mediante conductas inequívocas del titular o su representante legal, que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca.

Para que se entienda que hubo autorización mediante conducta inequívoca, se deberá demostrar como mínimo que al momento de recolectar la autorización se le informó al titular acerca de la existencia de la Política de Privacidad, la forma de acceder a ésta, las finalidades y tratamientos que se pretende dar a los datos personales, nombre o razón social y datos de contacto del responsable del tratamiento y derechos que le asisten como titular.

4.1.7. Conservación de la autorización

Sea cual sea la forma de obtención de la autorización, se debe conservar prueba de la existencia de la misma.

4.1.8. Política de Privacidad y Avisos de Privacidad

Todas las finalidades deberán estar incluidas en la Política de Privacidad, previo al uso de los datos personales o incluirse en Avisos de Privacidad.

Se deberán conservar todas las versiones de las políticas que se adopten, así como constancia de la publicación de cada una de ellas y la puesta en conocimiento de las mismas a los titulares.

En caso de haber cambios sustanciales en el contenido de la Política de Privacidad en relación con la identificación del responsable y las finalidades del tratamiento de los datos personales, estos deberán ser comunicados al titular y se deberá solicitar autorización previa, para usar los datos con las nuevas finalidades introducidas.

En los casos en los que no sea posible poner a disposición del Titular la Política de Privacidad, el operativo deberá informar al titular de manera oportuna y en todo caso a más tardar al momento de la recolección de los datos personales, por medio de un Aviso de Privacidad, el nombre o razón social y datos de contacto del responsable del tratamiento, existencia de dicha política y la forma de acceder ella, tratamiento al cual serán sometidos los datos y la finalidad del mismo, derechos que le asisten al titular.

En caso de recolectar datos sensibles, el Aviso de Privacidad deberá señalar expresamente el carácter facultativo de la respuesta a las preguntas que versen sobre este tipo de datos.

El responsable de bases de datos del área o proceso que recolecte la autorización, deberá garantizar la conservación del aviso de privacidad y autorización que utilice, y deberá velar porque se introduzca dentro de las tablas de retención documental este tipo documental, para efectos que el responsable del tratamiento conserve la evidencia de la autorización por el tiempo determinado en la valoración documental y de información personal.

Para el almacenamiento del aviso de privacidad y autorización, el responsable del tratamiento podrá emplear medios informáticos, electrónicos o cualquier otra tecnología que garantice el cumplimiento de lo previsto en la ley 527 de 1999, o las normas que la complementen, sustituyan, modifiquen o deroguen.

4.1.9. Preceptos

No se podrán utilizar medios engañosos o fraudulentos para recolectar y realizar tratamiento sobre datos personales.

En caso de que la recolección de datos personales la realice un encargado del tratamiento, se debe cumplir con lo dispuesto en el punto 4.4.2 del presente Manual.

4.2. ALMACENAMIENTO

Los datos personales podrán ser almacenados en medios físicos y/o magnéticos dentro o fuera del país, mientras subsista la finalidad para la cual se recolectaron, adoptando las medidas de seguridad requeridas para la protección de datos personales.

En caso de que el almacenamiento de datos personales la realice un encargado del tratamiento, se debe cumplir con lo dispuesto en el punto 4.4.2 del presente Manual.

4.3. USO

Para el uso de los datos personales de los titulares, se deberán tener en cuenta las siguientes indicaciones:

4.3.1. Finalidades autorizadas

Sólo se podrán usar los datos personales para las finalidades que hayan sido autorizadas por el titular o su representante, salvo las excepciones establecidas en las normas vigentes, incluyendo:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial
- Datos de naturaleza pública
- Casos de urgencia médica o sanitaria (siempre que no sea posible recolectar la autorización)
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos
- Datos relacionados con el Registro Civil de las personas
- Mandato legal o judicial que releve del consentimiento

Se deberá establecer un mecanismo para verificar qué finalidades autorizó el titular y cuáles no, o sobre cuáles el titular o su representante revocó su autorización.

4.3.2. Encargados del Tratamiento

En caso de que el uso de datos personales la realice un encargado del tratamiento, se debe cumplir con lo dispuesto en el punto 4.4.2 del presente Manual.

4.4. CIRCULACIÓN

La circulación de los datos personales, se realizará cumpliendo las siguientes reglas:

4.4.1. Circulación entre Operativos

Los operativos sólo podrán acceder o consultar la información o datos personales que reposen en las bases de datos del responsable del tratamiento cuando sea estrictamente necesario para el ejercicio de sus funciones o actividades encomendadas.

Los operativos podrán utilizar la información a la que tengan acceso para la ejecución de las labores y funciones asociadas a su cargo o actividad, por lo que les está prohibido usarla para fines distintos y deberán abstenerse de suministrarla, cederla o comercializarla a terceras personas naturales o jurídicas, públicas o

privadas, salvo que la misma sea de naturaleza pública sin sujeción a reserva, o sea requerida por una autoridad competente en el ejercicio de sus funciones legales, caso en el cual deberán avisar de inmediato al oficial de protección de datos personales, para que sea ésta quien defina cómo atender el requerimiento realizado por la autoridad competente.

4.4.2. Transmisión de datos personales

El responsable del tratamiento podrá encargar a una tercera persona natural o jurídica el tratamiento de datos personales de los titulares que componen sus grupos de interés, dentro o fuera del país.

Para los anteriores efectos, los operativos y responsables de bases de datos deberán velar porque se envíen cláusulas de transmisión de datos al momento de la transmisión, cuando quiera que con el tercero no se suscriba un contrato, y, en caso de que se suscriba un contrato, velar porque el área correspondiente suscriba un contrato de transmisión con el encargado del tratamiento. Tanto la cláusula como el contrato de transmisión, deberán contener como mínimo:

- Los alcances del Tratamiento.
- Las actividades que el encargado realizará por cuenta del responsable para el tratamiento de los datos personales y las obligaciones del encargado para con el titular y el responsable del tratamiento.
- La obligación de dar aplicación a las obligaciones del responsable del tratamiento bajo la Política de Privacidad, de acuerdo con la finalidad que los titulares hayan autorizado y con las leyes aplicables.
- La obligación de dar tratamiento, a nombre del responsable del tratamiento, a los datos personales conforme a los principios que los tutelan.
- La obligación de salvaguardar la seguridad de las bases de datos en los que se contengan datos personales.
- La obligación de guardar confidencialidad respecto del tratamiento de los datos personales.

En los casos en los que se realice algún tratamiento por parte de los encargados del tratamiento fuera del país, el país deberá contar con estándares seguros, de conformidad con lo dispuesto por la Superintendencia de Industria y Comercio, salvo las siguientes transmisiones:

- Información respecto de la cual el titular haya otorgado su autorización expresa e inequívoca para la transmisión;
- 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;
- Transmisiones acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad;
- Transmisiones 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;
- Transmisiones legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

Las transmisiones internacionales de datos personales que se efectúen entre el responsable del tratamiento y un encargado del tratamiento, para permitir que el encargado realice el tratamiento por cuenta del responsable del tratamiento, no requerirán ser informadas al titular ni contar con su consentimiento cuando exista entre ellos un contrato de transmisión de datos personales.

En aquellos casos en los que se transmitan datos personales a países no seguros y no se cuente con un contrato de transmisión de datos personales o se esté dentro de las excepciones establecidas en las normas vigentes, se deberá pedir la Declaratoria de Conformidad ante la Superintendencia de Industria y Comercio, de acuerdo con el procedimiento que esta entidad establezca.

Cuando quiera que, por la posición dominante del encargado del tratamiento, no sea posible exigir el cumplimiento de la Política de Privacidad del responsable del tratamiento, la suscripción de contratos o el envío de cláusulas de confidencialidad y transmisión de datos personales, se deberá garantizar que el tercero cuenta con políticas de privacidad adecuadas, que garanticen como mínimo la confidencialidad, disponibilidad e integralidad de la información.

4.4.3. Transferencia de datos personales

El responsable del tratamiento podrá realizar transferencia de datos personales a otros responsables del tratamiento, previa autorización del titular, salvo las excepciones establecidas en las normas vigentes, incluyendo:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial
- Datos de naturaleza pública
- Casos de urgencia médica o sanitaria (siempre que no sea posible recolectar la autorización)
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos
- Datos relacionados con el Registro Civil de las personas
- Mandato legal o judicial que releve del consentimiento

Cuando se realicen transferencias internacionales de datos personales, se debe verificar que el país al cual se transfieren los datos, cuente con niveles adecuados de protección de datos personales, conforme a los estándares que fije la Superintendencia de Industria y Comercio.

Lo anterior no aplica en los siguientes casos:

- Exista autorización previa y expresa del titular para la transferencia internacional;
- 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; o
- Se cuente con una Declaración de Conformidad expedida por la Superintendencia de Industria y Comercio.

Sin perjuicio de lo anterior, los operativos y responsables de bases de datos deberán velar porque se envíen cláusulas de transferencia de datos al momento de la transferencia, cuando quiera que con el tercero no se suscriba un contrato, y, en caso de que se suscriba un contrato, velar porque el área correspondiente suscriba un contrato de transferencia con el responsable del tratamiento receptor. Tanto la cláusula como el contrato de transferencia, deberán contener como mínimo:

- Los alcances del tratamiento, las actividades para las cuales se transfiere la información;
- La obligación del responsable del tratamiento receptor de cumplir con las normas de protección de datos personales y de dar tratamiento únicamente para las finalidades autorizadas por el titular en aplicación de los principios establecidos en las normas vigentes;
- La obligación de adoptar las medidas de seguridad que se requieran para proteger los datos personales y el deber de guardar estricta confidencialidad respecto del tratamiento de los datos Personales.

En aquellos casos en los que se transfieran datos personales a países no seguros y no se esté dentro de las excepciones establecidas en las normas vigentes, se deberá pedir la Declaratoria de Conformidad ante la Superintendencia de Industria y Comercio, de acuerdo con el procedimiento que esta entidad establezca.

4.4.4. Titulares y personas legitimadas

Los titulares, sus representantes o aquellas personas que se encuentren legitimadas por normas vigentes, pueden presentar peticiones, quejas, consultas y reclamos a través de los canales establecidos en la política de privacidad del responsable del tratamiento.

Las siguientes, son las personas facultadas para presentar PQR´s en ejercicio del Derecho de Hábeas Data, conforme con lo dispuesto por el artículo 2.2.2.25.4.1. del Decreto 1074 de 2015:

- El Titular, quien deberá acreditar su identidad en forma suficiente.
- Los causahabientes del Titular, quienes deberán acreditar tal calidad.
- El representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.
- Por estipulación a favor de otro o para otro, siempre que medie la aceptación por parte del Titular, de lo cual, se deberá presentar constancia en la solicitud.

Los derechos de los Niños, Niñas o Adolescentes se ejercerán por las personas que estén facultadas para representarlos.

Las peticiones y quejas, serán resueltas dentro de los términos establecidos en la Ley 1755 de 2015 o aquella que la sustituya, modifique o derogue.

Las consultas y reclamos serán resueltos dentro de los términos establecidos en las Leyes 1266 de 2008 y 1581 de 2012, o aquellas que las sustituyan, modifiquen o deroguen.

4.4.5. Consultas y reportes de información comercial, financiera, crediticia y de servicios (Ley 1266 de 2008)

Para realizar consultas y reportes de información comercial, financiera y crediticia ante los operadores de información, se deberá contar con la autorización previa del titular, que, para este caso específico, se consideran titulares tanto las personas naturales, como jurídicas.

El responsable del tratamiento o fuente de información, podrá realizar reportes positivos de los titulares en cualquier tiempo.

Para realizar reportes negativos ante los diferentes operadores de información, el responsable del tratamiento deberá enviar comunicación previa a los titulares con una antelación de veinte (20) días calendario, en la cual se le informe a este último de la mora presentada, para que el mismo pueda demostrar o efectuar el pago de la obligación, así como controvertir aspectos tales como el monto de la obligación o cuota y fecha de exigibilidad.

Pasados los veinte (20) días calendario antedichos, sin que el titular cancele las obligaciones pendientes o demuestre no ser deudor de la obligación, el responsable del tratamiento podrá realizar el reporte negativo respectivo.

En caso que el titular presente una solicitud de rectificación o actualización, el responsable del tratamiento deberá informar al operador de información que la información reportada se encuentra en discusión por parte del titular.

4.4.6. Requerimiento de información por autoridad administrativa o judicial competente

Cuando una autoridad administrativa o judicial competente requiera información personal, se deberá validar que en el requerimiento incluya:

- La norma que los faculta a requerir la información;
- La finalidad para la cual se requiere la información; y
- La forma en que debe ser enviada la información, para garantizar la protección de los Datos Personales.

4.5. ACTUALIZACIÓN

La actualización de datos personales se podrá llevar a cabo, en los siguientes casos:

4.5.1. Reclamo del titular o de personas legitimadas

En caso de reclamo, el Responsable del Tratamiento, a través del Oficial de protección de datos personales, deberá velar porque los operativos o responsables de bases de datos, actualicen la información dentro de los quince (15) días hábiles siguientes a la presentación del mismo, y los operativos directamente, o a través de los responsables de bases de datos, comunicarán de manera inmediata a los encargados del tratamiento (cuando aplique), todas las novedades respecto de los datos que previamente le haya suministrado, con el fin de garantizar que la información suministrada a estos últimos, se mantenga actualizada.

El encargado del tratamiento deberá actualizar la información dentro de los cinco (5) días hábiles siguientes a que el responsable del tratamiento le informe de la actualización.

4.5.2. Otros mecanismos de actualización

El Responsable del Tratamiento podrá implementar mecanismos tales como encuestas, campañas de actualización, cruce de información con bases de datos públicas, entre otras, previa autorización del titular, salvo las excepciones establecidas en las normas vigentes, incluyendo:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial
- Datos de naturaleza pública
- Casos de urgencia médica o sanitaria (siempre que no sea posible recolectar la Autorización)
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos
- Datos relacionados con el Registro Civil de las Personas
- Mandato legal o judicial que releve del consentimiento

4.5.3. Orden de autoridad administrativa o judicial competente

El responsable del Tratamiento deberá actualizar la información cuando así lo ordene una autoridad administrativa o judicial competente en el ejercicio de sus funciones.

Para efectos probatorios, deberá conservar copia del instrumento a través del cual la autoridad administrativa o judicial competente ordenó la actualización.

4.5.4. Encargado del Tratamiento

En caso de que la actualización de datos personales la realice un encargado del tratamiento, se debe cumplir con lo dispuesto en el punto 4.4.2 del presente Manual.

4.6. SUPRESIÓN O DISPOSICIÓN FINAL

4.6.1. Principios

La supresión de los Datos Personales se relaciona con los siguientes Principios:

PRINCIPIO DE FINALIDAD: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.

PRINCIPIO DE CADUCIDAD: Prohíbe la conservación indefinida de datos después de que han desaparecido las causas que justificaban su administración.

4.6.2. Casos en los que procede:

La supresión de los datos personales deberá realizarse en los siguientes casos, inmediatamente al momento de cumplirse alguno de los siguientes supuestos:

4.6.2.1. Culminación finalidad

El responsable del tratamiento y los encargados del tratamiento podrán tratar los datos personales mientras subsistan las finalidades para las cuales fueron recolectados, y atendiendo aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.

Una vez cumplida la o las finalidades para las cuales se recolectaron los datos, el responsable del tratamiento y el encargado del tratamiento, deberán proceder a la supresión de los mismos, salvo que se requiera su conservación para el cumplimiento de una obligación legal o contractual.

4.6.2.2. Revocatoria de autorización o reclamo de supresión

En caso de revocatoria de la autorización o reclamo de supresión, el responsable del tratamiento deberá suprimir la información dentro de los quince (15) días hábiles siguientes a la presentación del mismo, comunicando de forma oportuna al encargado del tratamiento, la obligación de suprimir los datos.

El término anterior podrá extenderse por ocho (8) días más, siempre que se informen al interesado las causas de la demora y la nueva fecha para resolver su reclamo.

El encargado del tratamiento deberá suprimir la información dentro de los cinco (5) días hábiles siguientes a que el Responsable del Tratamiento le comunique la obligación de supresión.

La solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el Titular tenga un deber legal o contractual de permanecer en la base de datos; la eliminación de datos obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas; o los datos sean necesarios para proteger los intereses jurídicamente tutelados del titular para realizar una acción en función del interés público o para cumplir con una obligación legalmente adquirida por el titular.

4.6.2.3. Orden de autoridad administrativa o judicial competente

El responsable del tratamiento deberá suprimir la información cuando así lo ordene una autoridad administrativa o judicial competente, en el ejercicio de sus funciones.

Para efectos probatorios, deberá conservar copia del instrumento a través del cual la autoridad administrativa o judicial competente ordenó la eliminación.

4.6.2.4. Definición de tiempos de Retención de Datos Personales

El responsable del tratamiento deberá definir el tiempo que desea conservar los documentos e información que contenga datos personales.

Los tiempos de retención, serán los contenidos en las tablas de retención documental, las cuales se adoptarán, en atención a los:

1. Tiempos establecidos por orden legal o judicial;
2. Tiempos definidos por el responsable del tratamiento para los documentos o datos personales de conformidad con las valoraciones realizadas por la entidad.

Los tiempos definidos para los documentos de acuerdo con la valoración realizada por la entidad, no podrán en ningún momento ser inferiores a los tiempos establecidos por orden legal o judicial y podrán ser superiores, siempre y cuando la decisión de definir un tiempo superior, esté debidamente fundamentada.

4.6.3. Documentación de la supresión o disposición final

La supresión de los datos personales deberá quedar consignada en un acta debidamente firmada por el oficial de protección de datos personales del responsable del tratamiento y por el o los operativos o responsables de la base de datos de la cual se suprime el dato personal.

4.6.4. Encargado del Tratamiento

En caso de que la supresión de datos personales la realice un encargado del tratamiento, se debe cumplir con lo dispuesto en el punto 4.4.2 del presente Manual.

Asimismo, deberá quedar consignada un acta debidamente firmada por el Oficial de protección de datos personales del responsable del tratamiento y por el encargado del tratamiento o por quienes éste designe para llevar a cabo dicha labor.

5. INCIDENTES DE SEGURIDAD O VIOLACIONES A LAS NORMAS DE PROTECCIÓN DE DATOS PERSONALES

Los operativos directamente, o a través del responsable de base de datos designado para su área o proceso, y los encargados del tratamiento, deberán informar por escrito al oficial de protección de datos personales inmediatamente a su materialización o al momento en que llegaren a su conocimiento, la

ocurrencia de cualquier incidente de seguridad o violación a las normas de protección de datos personales, indicando sus posibles causales y tipos, junto con la descripción de los hechos conocidos.

5.1. CAUSALES DE LOS INCIDENTES DE SEGURIDAD O VIOLACIONES A LAS NORMAS DE PROTECCIÓN DE DATOS PERSONALES

Las causas por las que se pueden presentar incidentes de seguridad o violaciones a las normas de protección de datos personales, son las siguientes:

Causal	Descripción
Fraude interno	Delito efectuado con la participación de los empleados o personas de confianza del responsable o encargado del tratamiento, bien sea en forma directa o indirecta
Fraude externo	Cualquier acto efectuado por una persona ajena al responsable o encargado del tratamiento, buscando acceder, apropiarse, causar adulteración o eliminación a los datos personales a los cuales estos les realizan tratamiento
Daños a activos físicos	Pérdida, deterioro o cualquier afectación de los datos personales a los cuales el responsable o encargado realicen tratamiento, causados por daños a los activos físicos de los mismos
Caso fortuito	Evento de la naturaleza que es impredecible, en virtud de la cual se presente la pérdida, indisponibilidad, adulteración o cualquier afectación de los datos personales a los cuales el responsable o encargado realicen tratamiento
Falla de tecnología informática	Pérdida, indisponibilidad, adulteración o cualquier afectación de los datos personales a los cuales el responsable o encargado realicen tratamiento, causados por fallas en la infraestructura tecnológica de uno u otro
Fallas en la ejecución y/o administración de procesos o defectos en los mismos	Pérdida, indisponibilidad, adulteración o cualquier afectación de los datos personales a los cuales el responsable o encargado realicen tratamiento, causados por fallas en la ejecución, aplicación y/o administración de procesos, procedimientos, protocolos, políticas de uno u otro, o defectos en los mismos
Falla por negligencia o actos involuntarios de los titulares	Pérdida, indisponibilidad, adulteración o cualquier afectación de los datos personales a los cuales el responsable o encargado realicen tratamiento, causados por negligencia o actos involuntarios del mismo titular, que puede ver afectados tanto sus propios datos como los de otros titulares

5.2. TIPOS DE INCIDENTES DE SEGURIDAD O VIOLACIONES A LAS NORMAS DE PROTECCIÓN DE DATOS PERSONALES

Los tipos de incidentes de seguridad o violaciones a las normas de protección de datos personales que se pueden presentar, son los siguientes:

Tipo de incidente	Descripción
Afecta la confidencialidad de los datos personales	Todos aquellos incidentes que afecten el principio de seguridad relacionado con la confidencialidad de los datos personales, siendo ésta, la característica que evita la divulgación de la información a personas o procesos que no estén debidamente autorizados
Afecta la disponibilidad de los datos personales	Todos aquellos incidentes que afecten el principio de seguridad relacionado con la disponibilidad de los datos personales, que es la característica que garantiza el acceso a la información por las personas o procesos autorizados, siempre que sea requerida
Afecta la integralidad de los datos personales	Todos aquellos incidentes que afecten el principio de seguridad relacionado con la integralidad de la información, que es la característica que garantiza que la información no se fraccione o deteriore

5.3. CONFORMACIÓN DEL EQUIPO DE TRABAJO PARA LA ACTIVACIÓN DEL PROTOCOLO DE INCIDENTES DE SEGURIDAD O VIOLACIÓN A LAS NORMAS DE PROTECCIÓN DE DATOS PERSONALES

Una vez llegue a conocimiento del oficial de protección de datos personales la ocurrencia de un incidente de seguridad y/o violación a las normas de protección de datos personales, deberá proceder con la conformación del equipo de trabajo para la activación del protocolo de incidentes de seguridad, el cual deberá estar conformado como mínimo por:

- Un delegado del Área de Servicio al Cliente, en calidad de Oficial de protección de datos personales.
- El o los responsables de bases de datos de las bases de datos posiblemente afectadas por el incidente de seguridad.

El equipo de trabajo para la activación del protocolo de incidentes de seguridad se constituirá de acuerdo con la necesidad puntual y podrán invitarse terceros que, por sus conocimientos y competencias, puedan colaborar en el análisis y evaluación del incidente, su contención, los riesgos asociados al mismo y los daños potenciales a los titulares o terceros.

5.4. FUNCIONES DEL EQUIPO DE TRABAJO PARA LA ACTIVACIÓN DEL PROTOCOLO DE INCIDENTES DE SEGURIDAD Y/O VIOLACIÓN DE LAS NORMAS DE PROTECCIÓN DE DATOS PERSONALES

El equipo de trabajo para la activación del protocolo de incidentes de seguridad deberá:

5.4.1. Analizar y evaluar el incidente de seguridad/violación a las normas de protección de datos personales

El equipo de trabajo para la activación del protocolo de incidentes de seguridad y/o violación a las normas de protección de datos personales, realizará la investigación correspondiente para establecer:

- ¿Es un incidente de seguridad o violación de las normas que rigen la protección de datos personales? (En caso afirmativo continuar con los siguientes interrogantes)
- ¿Cómo se produjo el incidente de seguridad y/o la violación a las normas de protección de datos personales?
- ¿Cuándo y dónde tuvo lugar?
- ¿Cuál fue la causal y quién lo detectó?
- ¿Fue un hecho aislado o persisten las causales que generaron el incidente de seguridad o violación a las normas de protección de datos personales?
- ¿Qué se puede hacer para asegurar la contención del incidente de seguridad y/o violación a las normas de protección de datos personales y reducir el riesgo de daños a los titulares o terceros afectados?
- ¿Qué se puede hacer para asegurar que el incidente de seguridad y/o la violación a las normas de protección de datos personales no vuelva a presentarse en el futuro?
- ¿El incidente de seguridad debe ser notificado a los Titulares o personas afectadas para que estas lleven a cabo acciones que eviten la generación de un daño?

5.4.2. Acciones para contener el incidente de seguridad y/o violación a las normas de protección de datos personales y reducir el riesgo de daños a los titulares o terceros que puedan verse afectados

El equipo de trabajo para la activación del protocolo de incidentes de seguridad y/o violación a las normas de protección de datos personales, deberá establecer las actividades necesarias para la contención del incidente de seguridad y/o violación, y reducir el riesgo de daños a los titulares o terceros que puedan verse afectados, asignando para tales efectos responsables para el cumplimiento de cada actividad y la fecha máxima para su ejecución.

En caso de imposibilidad para el cumplimiento de alguna(s) de las actividades asignadas, el/los responsables para el cumplimiento de la actividad, convocarán(n) nuevamente al equipo de trabajo para la activación del protocolo de incidentes de seguridad y/o violación, para el análisis de otras alternativas para la contención del incidente de seguridad y reducir el riesgo de daños a los titulares o terceros que puedan verse afectados.

5.4.3. Evaluación de riesgos e impactos

El equipo de trabajo para la activación del protocolo de incidentes de seguridad y/o violación a las normas de protección de datos personales, deberá realizar el análisis de riesgos e impactos de acuerdo con la metodología que para los efectos disponga la compañía.

Dentro de dicha evaluación, se analizará como mínimo:

5.4.3.1. Respecto de la información

- Volumen de Datos Personales afectados
- Tipo de datos personales afectados y su naturaleza (datos públicos, datos semiprivados, datos privados y/o datos sensibles)
- Cómo se puede utilizar la información personal afectada en caso de acceso no autorizado o fraudulento por parte de terceros (ejemplo: Se puede utilizar la información personal para fines fraudulentos o puede causar cualquier tipo de daño material y/o inmaterial al titular o terceros.)
- ¿Se ha recuperado la información personal?

5.4.3.2. Respecto de los Titulares o terceros

- Estimación de la cantidad de personas que pudieron verse afectadas
- Identificación del/los grupos de interés a los que pertenecen las personas que pudieron verse afectadas
- Situación de las personas que pudieron verse afectadas (Ejemplo: Niños, Niñas y/o Adolescentes, personas en estado de vulnerabilidad o en situación de discapacidad, etc.)
- Posibles daños generados (Por ejemplo: Riesgo en su seguridad física o psicológica, extorsión económica o sexual, hurto o suplantación de identidad, pérdida financiera, negación de un crédito o seguro, perfilamiento con fines ilícitos, pérdida de negocios u oportunidades de empleo, discriminación, humillación significativa o pérdida de dignidad o daño a la reputación, riesgo para la salud o seguridad pública, pánico económico).

5.4.3.3. Respecto de la organización

- Posibles daños generados (Por ejemplo: Pérdida reputacional, pérdida de clientes o usuarios, pérdida de confianza en la organización, honorarios de consultores e ingenieros forenses, pérdida de activos, sanciones, órdenes e instrucciones administrativas y/o judiciales, exposición financiera).

5.4.4. Comunicación a los Titulares o terceros afectados

En caso de identificarse la necesidad, el equipo de trabajo para la activación del protocolo de incidentes de seguridad deberá notificar a los titulares y terceros que se vean afectados con el incidente de seguridad respecto de la ocurrencia del mismo, las posibles consecuencias y la orientación respecto de las medidas que pueden adoptar para efectos de minimizar los posibles daños.

Para los anteriores efectos, el equipo de trabajo determinará cuándo, cómo, a quién, e información que debe incluirse en la notificación.

5.4.5. Establecimiento de acciones correctivas

El equipo de trabajo para la activación del protocolo de incidentes de seguridad y/o violaciones a las noemas de protección de datos personales, deberá establecer las actividades correctivas necesarias para evitar que el incidente de seguridad vuelva a presentarse, asignando para tales efectos responsables para el cumplimiento de cada actividad y la fecha máxima para su ejecución.

En caso de imposibilidad para el cumplimiento de alguna(s) de las actividades asignadas, el/los responsables para el cumplimiento de cada actividad, convocará(n) nuevamente al Equipo de trabajo, para el análisis de otras alternativas para mitigar los riesgos asociados al incidente de seguridad y/o violación a las normas de protección de datos analizada.

5.4.6. Reporte del incidente de seguridad a la Superintendencia de Industria y Comercio

El Oficial de protección de datos personales reportará, dentro de los términos establecidos en las normas vigentes, los incidentes de seguridad que se presenten en materia de datos personales y en la forma que defina esta entidad o la que asuma sus funciones.

5.4.7. Documentación

El equipo de trabajo para la activación del protocolo de incidentes de seguridad y/o violaciones a las normas de protección de datos personales, deberá dejar debidamente documentadas y soportadas todas las actividades realizadas en relación con el incidente de seguridad y/o violaciones a las normas de protección de datos personales, definidas en los puntos anteriores.

6. REPORTES QUE DEBEN REGISTRARSE ANTE EL RNBD ADMINISTRADA POR LA SIC

Los siguientes, son los reportes que deben presentarse ante la SIC:

6.1. INSCRIPCIÓN DE NUEVAS BASES DE DATOS

Las áreas o procesos que creen nuevas Bases de Datos, deberán informar dicho hecho al Oficial de Protección de Datos Personales, quien se encargará de incluir la misma en el Inventario de Bases de Datos y designará un Responsable de la Base de Datos.

Las Bases de Datos que se creen, deberán inscribirse en el RNBD, dentro de los dos (2) meses siguientes a su creación, por parte del Responsable de la Base de Datos.

El Oficial de Protección de Datos Personales velará por el cumplimiento del término para hacer el registro y podrá realizar auditorías al mismo, para verificar que se haya realizado en debida forma.

6.2. ACTUALIZACIÓN DE INFORMACIÓN DE BASES DE DATOS REGISTRADAS

Los Responsables de Bases de Datos previamente inscritas en el RNBD, deberán informar al Oficial de Protección de Datos Personales todas las modificaciones que se realicen a las mismas, inmediatamente.

El Oficial de Protección de Datos Personales actualizará el Inventario de Bases de Datos y exhortará al Responsable de la Base de Datos para que reporte las actualizaciones en el RNBD, en los siguientes términos:

i. Cuando los cambios sean sustanciales (entendidos estos por cambios en finalidades, Encargados del Tratamiento, canales de atención de Consultas y Reclamos, tipos de datos personales almacenados en las Bases de Datos, medidas de seguridad implementadas, Política de Datos Personales, o transferencia o transmisión internacional de datos personales), el reporte se deberá realizar dentro de los primeros diez (10) días hábiles de cada mes, cuando se realicen cambios;
ii. Cuando los cambios no sean sustanciales, el reporte se deberá realizar anualmente entre el 02 de enero y el 31 de marzo.

6.3. RECLAMOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

El Oficial de Protección reportará en el RNBD los Reclamos que se presenten en materia de Protección de Datos Personales semestralmente, en los siguientes términos:

i. Reclamos presentados de enero a junio, dentro de los primeros quince (15) días hábiles del mes de agosto; y
ii. Reclamos presentados de julio a diciembre, dentro de los primeros quince (15) días hábiles del mes de febrero.

6.4. INCIDENTES DE SEGURIDAD O VIOLACIONES A LAS NORMAS DE PROTECCIÓN DE DATOS PERSONALES

El Oficial de Protección de Datos Personales deberá reportar en el RNBD los incidentes presentados, dentro de los quince (15) días hábiles siguientes a que se detecten los mismos.

El Responsable del Tratamiento deberá comunicar a los Titulares afectados la ocurrencia de los incidentes, buscando una compensación por los daños que pudieren causarse.

El Oficial de Protección de Datos Personales, deberá guardar registro de las actividades llevadas a cabo al momento de identificar la materialización del incidente de seguridad o la violación a las normas que regulan la Protección de Datos Personales y de las medidas adoptadas para evitar la propagación del incidente o de la vulneración.