MANUAL: PROTECCION DE DATOS PERSONALES IDPC

PROCESO: ATENCIÓN A LA CIUDADANÍA TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA

Versión: 1 del 2 de Octubre de 2023

Contenido

1. ANTECEDENTES

La creación del manual de protección de datos personales en el Instituto Distrital de Patrimonio Cultural, tiene como necesidad la articulación del “hacer” en la gestión de la protección de datos personales; gestión ya plasmada en el documento de la Política de Protección de Datos Personales de IDPC.

En este sentido dicho manual, es esencial para garantizar el seguimiento de los procedimientos de la privacidad y seguridad del dato personal. Dado que la protección de los datos personales es una prioridad importante en el IDPC, un manual de este tipo debe establecer procedimientos detallados y medidas de seguridad necesarias, para garantizar la protección de los datos personales y el cumplimiento de las regulaciones legales[1].

La necesidad del IDPC en cumplir con la responsabilidad demostrada en el tratamiento de datos personales[2], también es conocida como accountability, se refiere a implementar estrategias que permitan demostrar que se están cumpliendo con todas las regulaciones y normas establecidas, en materia de privacidad y seguridad de la información personal. Se trata de un enfoque preventivo, que busca minimizar los riesgos relacionados con el manejo de los datos personales y garantizar su protección. Es por ello que es importante que las entidades implementen medidas de seguridad adecuadas y que capaciten a sus funcionarios en el correcto manejo de la información personal, para garantizar el cumplimiento de la responsabilidad demostrada establecida en el Decreto 1377 de 2013.

Además, el manual de protección de datos personales ayudará a promover la cultura de protección de datos en toda la organización, garantizando que todos los funcionarios involucrados en el manejo de datos personales, estén debidamente capacitados y preparados para manejar información personal con seguridad y privacidad.

En definitiva, debemos dentro del manual, hacer una breve síntesis de la política de protección de datos con el fin, de poder entender el “hacer” de la gestión de datos:

[1] El artículo 15 de la Constitución Política de Colombia.
[2] Capítulo VI responsabilidad demostrada frente al tratamiento de datos personales Decreto 1377 del 2013.

1.1. Políticas de Operación

La política de operación del tratamiento de datos personales en IDPC, describe los procedimientos y medidas de seguridad necesarias para garantizar la protección de los datos personales recolectados, usados, almacenados y procesados. Esta política establece los derechos y las obligaciones de los titulares de datos y los responsables del tratamiento de los mismos, en cumplimiento con las leyes y regulaciones colombianas en materia de protección de datos personales, tales como la Ley 1581 de 2012. También establece los procedimientos necesarios para asegurar el ejercicio efectivo de los derechos de consulta, actualización, rectificación y supresión.

1.2. Política de Protección de Datos Personales

De acuerdo con lo establecido en la política de Protección de Datos Personales, del Instituto Distrital de Patrimonio Cultural, la protección de datos personales es una prioridad importante, y se rige por la Ley de Protección de Datos Personales 1581 de 2012. Esta ley establece los lineamientos para el tratamiento de la información personal, incluyendo la recolección, uso, almacenamiento y procesamiento de los datos personales dentro del territorio colombiano. Esta ley también establece los derechos y obligaciones de los titulares de los datos y los responsables del tratamiento de los mismos, y establece los procedimientos necesarios para el cumplimiento de las obligaciones legales en materia de protección de datos personales.

La política de protección de datos personales en Colombia debe cumplir con los lineamientos establecidos en la Ley 1581 de 2012, y debe establecer los procedimientos y medidas de seguridad necesarios para garantizar la protección de la información personal recolectada. Esta política debe garantizar el ejercicio efectivo de los derechos (consulta, actualización, rectificación y supresión) y establecer los mecanismos necesarios para su cumplimiento. Además, la política de protección de datos personales debe ser conocida y adoptada, por todos los funcionarios involucrados en el manejo de datos personales dentro del IDPC, asegurando que se promueva la cultura de protección de datos y que se garantice la privacidad y la seguridad de la información personal de los ciudadanos colombianos.

1.3. Principios en el tratamiento de datos personales

Todas las entidades públicas o privadas, que realicen tratamiento de datos personales están obligadas a aplicar los principios y disposiciones establecidos en la Ley 1581 de 2012. Asimismo, la entidad responsable del tratamiento de los datos personales, debe implementar los controles necesarios para garantizar la protección de los datos personales y el cumplimiento de la ley en relación al tratamiento de los mismos.

1.3.1. El principio de legalidad

En la Ley 1581 de 2012 hace referencia a que el tratamiento de datos personales, solo podrá llevarse a cabo en aquellos casos en los que exista autorización previa, expresa e informada por parte del titular del dato o cuando se cuente con una autorización legal para ello. Es decir, el tratamiento de datos personales, debe estar ajustado a la ley y a los principios establecidos en la normativa, garantizando la protección de los derechos de los titulares de los datos. Este principio busca evitar el uso indiscriminado de datos personales y proteger la privacidad de las personas, asegurando que los datos sean recolectados, almacenados, usados y divulgados de forma adecuada y en cumplimiento con lo establecido en la normativa aplicable. En síntesis, el principio de legalidad, busca garantizar la protección de los derechos de los titulares de los datos y evitar el uso indebido o arbitrario de la información personal.

1.3.2. El principio de finalidad

La Ley 1581 de 2012, indica que el tratamiento de datos personales debe estar orientado a una finalidad legítima y explícita, previamente informada al titular del dato. Esto significa que la recolección, almacenamiento, uso y divulgación de los datos personales, debe estar enfocada en una finalidad específica y no se debe realizar un tratamiento distinto de aquel para el cual se obtuvo la autorización del titular del dato. Este principio busca evitar la utilización de datos personales, para fines diferentes a aquellos para los cuales se recolectaron y evitar la divulgación de información, sin el debido consentimiento del titular. La finalidad debe ser comunicada al titular de los datos, de forma clara y explícita para que pueda tomar una decisión fundamentada sobre la autorización del tratamiento de sus datos. En conclusión, el principio de finalidad establece, que el tratamiento de datos personales solo podrá ser realizado para una finalidad específica y legítima, informada previamente al titular del dato y autorizada por él.

1.3.3. El principio de libertad

El principio dicta que el tratamiento de datos personales, solo puede ser llevado a cabo con el consentimiento previo, expreso e informado del titular del dato. Esto significa que los datos personales no pueden ser tratados sin la autorización del titular y que éste tiene el derecho de autorizar el tratamiento de sus datos de forma específica e informada. La Ley 1581 de 2012, también establece que los datos personales no pueden ser utilizados para fines distintos, a aquellos para los que se obtuvo el consentimiento. En resumen, el principio de libertad, garantiza que los derechos de los titulares de los datos, sean respetados y que el tratamiento de sus datos personales se realice de manera legítima y con su consentimiento previo e informado.

1.3.4. El principio de veracidad

El principio de veracidad determina que la información sometida a tratamiento debe ser veraz, completa, exacta y actualizada. Esto significa que los responsables del tratamiento de datos personales, deben asegurarse de que la información recolectada y almacenada es precisa y está actualizada para garantizar su calidad. El principio de veracidad busca proteger los derechos de los titulares de los datos y evitar la difusión de información falsa o inexacta.

1.3.5. El principio de transparencia

En la Ley 1581 de 2012, indica que en el tratamiento de datos personales se debe garantizar el derecho del titular a obtener del responsable del tratamiento o del encargado del tratamiento, información sobre los datos personales que le conciernen. Además, este principio, busca garantizar la accesibilidad de la información, relacionada con el tratamiento de los datos personales a los titulares, así como informarles sobre sus derechos y las políticas de tratamiento de la información. En síntesis, el principio de transparencia busca promover la divulgación y el acceso a la información sobre el tratamiento de los datos personales garantizando la protección de los derechos de los titulares de los datos.

1.3.6. El principio de acceso y circulación restringida

El tratamiento de datos personales, está sujeto a límites derivados de la naturaleza de dichos datos, los derechos de los titulares y las garantías constitucionales. Este principio plantea que los datos personales no pueden ser tratados o divulgados sin la autorización previa y expresa de los titulares de los

mismos, salvo excepciones contempladas en la ley. Además, busca garantizar que los datos personales tratados, sean accesibles únicamente para aquellos que tienen autorización para hacerlo, y que se apliquen medidas de seguridad para evitar el acceso no autorizado o la circulación excesiva de la información personal. En resumen, el principio de acceso y circulación restringida busca proteger la privacidad y los derechos de los titulares de los datos personales, limitando el tratamiento y la divulgación de la información a los casos autorizados por la ley.

1.3.7. El principio de seguridad

Este principio busca garantizar, que la información sujeta a tratamiento por el responsable del tratamiento o el encargado del tratamiento de los datos personales, sea manejada con las medidas técnicas, humanas y administrativas necesarias para garantizar su seguridad y privacidad. De esta manera, se pretende evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Abreviado, el principio de seguridad restringida busca proteger la privacidad y los derechos de los titulares de los datos personales, mediante la implementación de medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información.

1.3.8. El principio de confidencialidad

Todas las personas que intervengan en el tratamiento de los datos personales, que no tengan la naturaleza pública, están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de la misma. En resumen, el principio de confidencialidad busca proteger la privacidad y los derechos de los titulares de los datos personales mediante la obligación de mantener la reserva de la información, excepto en los casos establecidos por la ley y en los términos de la misma.

1.4. Corolario

Como conclusión de los antecedentes se puede decir que:

- El manual se origina de una necesidad de “hacer” de la política.
- La política tiene procedimientos de derechos y obligaciones, cumplimiento, seguridad, rectificación, almacenamiento.

- Todo funcionario puede consultar la política completa en el portal de la entidad: Pagina web de idpc.gov.co Política de Tratamiento de Datos Personales https://idpc.gov.co/politica-de-proteccion-de-datos-personales/
- En este sentido ahora sí podemos, después de esta pequeña exposición aclaratoria de la naturaleza y su articulación, entrar en materia para describir y explicar dicho manual de protección de datos.

2. OBJETIVO

Establecer los lineamientos y procedimientos necesarios que permitan garantizar la confidencialidad, integridad, disponibilidad y privacidad de los datos personales que sean objeto de tratamiento, con el fin de cumplir con las disposiciones establecidas en la normativa vigente[3]. Además, busca concientizar a los funcionarios sobre la importancia de proteger sus datos personales y brindarles herramientas y recomendaciones para que puedan hacerlo de manera efectiva.

3. ALCANCE

El alcance de este manual de protección de datos personales se refiere a la descripción detallada de los procedimientos, política y prácticas que se deben seguir para garantizar la protección y privacidad de los datos personales que sean objeto de tratamiento. Este manual sigue las normas y directrices necesarias para que el IDPC, pueda cumplir con la normativa, con la responsabilidad demostrable aplicable en materia de protección de datos y se aplique a todas las bases de datos y demás instrumentos que, en cumplimiento de sus procesos misionales, el IDPC realice tratamiento a datos personales.

4. DEFINICIONES

Dato Personal: Se entiende por datos sensibles, aquellos que afectan la intimidad del titular 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

[3] Decreto 1377 de 2013, Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

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.

Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

Aviso de privacidad: Comunicación verbal o escrita generada por el responsable, dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.

Base de datos: Conjunto organizado de datos personales que sea objeto de Tratamiento.

Información efectuada por daño a los intereses públicos: Es toda aquella información pública reservada, cuyo acceso podrá ser rechazado, denegado de manera motivada y por escrito en las siguientes circunstancias, siempre que dicho acceso estuviere expresamente prohibido por una norma legal o constitucional: La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva Ia medida de aseguramiento o se formule pliego de cargos, según el caso, la estabilidad macroeconómica y financiera del Instituto.

Habeas Data: Se denomina el derecho que tiene toda persona de conocer, corregir o actualizar toda aquella información que se relacione con ella y que se encuentre almacenada en centrales de información o bases de datos de organismos tanto públicos como privados.

Titular: Persona natural cuyos datos personales sean objeto de tratamiento.

Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

5. NORMATIVIDAD

Con la determinación de dar un apropiado tratamiento a los datos personales, el Instituto Distrital de Patrimonio Cultural ha identificado el siguiente marco normativo, que articula las disposiciones de protección de los datos personales, su confidencialidad y los derechos de los titulares:

- Constitución Política de 199, artículo 15.
- Decreto 1377 del 2013: Tiene como objeto reglamentar parcialmente la ley 1581 de la cual disposiciones generales para la protección de datos personales.
- Ley 1266 de 2008: Por la cual se dictan disposiciones generales del habeas 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 provenientes de terceros países, y se dictan otras disposiciones.
- Ley 1581 de 2012, hoy Decreto 1074 de 2015 y demás decretos reglamentarios que definan el ámbito de aplicación en los derechos a la intimidad, el buen nombre y la autodeterminación informativa.
- Ley 1712 de 2014 por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Decreto 103 de 2015 por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Sentencia C- 1011 de 2008 - Definición de la naturaleza del dato asentado en los Registros Públicos de las Cámaras de Comercio, como dato público.
- Sentencia C - 748 de 2011 - Constitucionalidad del proyecto de Ley Estatutaria de Protección de Datos Personales.
- Circular Externa 005 de 2017 de la Superintendencia de Industria y Comercio: Por la cual se fijan estándares de un nivel adecuado de protección en el país receptor de la información personal.
- Circular Externa 008 de 2017 de la Superintendencia de Industria y Comercio: Por la cual se incluye un país en la lista de aquellos que cuentan con un nivel adecuado de protección de datos personales.
- Guía de la Superintendencia de Industria y Comercio para la implementación del Principio de Responsabilidad Demostrada (Accountability).
- En general, para la aplicación e interpretación del presente manual, cuando fuere procedente, se aplicarán las demás normas que regulen o complementen lo concerniente a la protección de datos personales.

6. LINEAMIENTO DE OBTENCIÓN DE LA AUTORIZACIÓN

Son los lineamientos que deben seguirse para obtener la autorización previa, expresa e informada del titular de los datos para el tratamiento de información

personal. La norma establece que **la autorización debe ser otorgada por escrito, por cualquier otro medio que permita su almacenamiento, posterior consulta y debe ser solicitada por el responsable del tratamiento de los datos en este caso el IDPC, quien deberá informar al titular sobre el tratamiento al que serán sometidos sus datos personales.**

Además, el titular tiene derecho a revocar la autorización en cualquier momento, siempre y cuando no exista una obligación legal o contractual que impida su revocatoria. En caso de recibir la solicitud de revocatoria, el responsable del tratamiento, deberá proceder a la supresión de los datos personales, excepto en aquellos casos en los que deban conservarse debido a una obligación legal o contractual. El incumplimiento de las normas establecidas en el Decreto 1377 del 2013 puede conllevar sanciones y multas por parte de las autoridades correspondientes.

6.1. Autorización en formatos

La autorización previa para el tratamiento de datos personales, debe ser otorgada por el titular de los datos de manera expresa e informada. Para esto, se pueden utilizar los formatos modelo suministrados por la Superintendencia de Industria y Comercio (SIC) para facilitar el cumplimiento de la Ley 1581 de 2012 y garantizar el debido proceso. Los formatos deben incluir la información necesaria para que el titular de los datos, pueda conocer y autorizar el tratamiento al que están siendo sometidos sus datos personales, así como los derechos y mecanismos que tiene para hacerlos valer en caso de ser necesario. Es importante que la autorización se obtenga antes de iniciar el tratamiento de los datos y que se maneje de forma responsable y segura, en conformidad con las disposiciones del Decreto 1377 de 2013.

6.2. Autorización en formatos web

Los procesos que lleven a cabo iniciativas, que impliquen la recolección de datos personales a través de formularios web, deberán tener en cuenta los siguientes aspectos necesarios para su captura:

a) Solicitar sólo aquellos datos personales pertinentes conforme con la finalidad del tratamiento.

b) Relacionar en el formato, un aviso de privacidad, que incorpore la autorización del tratamiento por parte del titular.
c) El envío de la información a través del formulario, deberá estar condicionado a la previa aceptación de la autorización de tratamiento de los datos.
d) Validar que en el aviso de privacidad se encuentren todas las finalidades de tratamiento, asociadas a la captura de los datos personales requeridos por el IDPC.
e) Validar que la plataforma que soporta el formulario web tenga la capacidad técnica, operativa y de seguridad para almacenar las autorizaciones, y poder tener la trazabilidad en ellas.

6.3. Autorización en formatos físicos

Los procesos que lleven a cabo iniciativas que impliquen la recolección de datos personales a través de formularios físicos, deberán tener en cuenta los siguientes aspectos necesarios para su captura:

a) Solicitar sólo aquellos datos personales pertinentes conforme con la finalidad del tratamiento.
b) Relacionar en el formato, un aviso de privacidad que incorpore la autorización del tratamiento por parte del titular.
c) El envío de la información a través del formulario, deberá estar condicionado a la previa aceptación de la autorización de tratamiento de los datos.
d) Validar que en el aviso de privacidad se encuentren todas las finalidades de tratamiento asociadas a la captura de los datos personales requeridos por el IDPC.
e) Garantizar la custodia de los formularios con sus respectivas autorizaciones.

6.4. Contenido del aviso de privacidad

El Decreto 1377 de 2013 establece los requisitos y lineamientos para la creación de un aviso de privacidad, que debe ser proporcionado a los titulares de los datos personales. El aviso de privacidad debe contener información clara y detallada sobre el tratamiento al que serán sometidos los datos personales, incluyendo la finalidad del tratamiento, los derechos que tienen los titulares de los datos, los mecanismos para hacer valer esos derechos y las políticas de protección de datos que se implementan en la organización responsable del tratamiento.

El aviso de privacidad debe ser presentado de manera clara y accesible, en un lenguaje que sea fácilmente comprensible para el titular de los datos personales. Además, el aviso de privacidad debe ser proporcionado antes de que se inicie el tratamiento de los datos personales, para que el titular tenga la posibilidad de conocer y autorizar el tratamiento de sus datos de manera informada. El incumplimiento de las normas puede conllevar sanciones y multas por parte de las autoridades correspondientes.

6.5. Ejemplo de un aviso de privacidad

Aviso de privacidad:

El Instituto Distrital de Patrimonio Cultural, en cumplimiento de la Ley 1581 de 2012 y normas vinculantes, es responsable del tratamiento de sus datos personales. Para conocer las políticas, puede consultar en la página de internet: https://idpc.gov.co/politica-de-proteccion-de-datos-personales/. Los datos personales solicitados tienen la siguiente finalidad: Gestión de documentos para usuarios internos y externos, que soliciten algún tipo de préstamo documental de la entidad. En calidad de titular de la información el Instituto, tiene derecho a conocer, actualizar y rectificar sus datos personales, y sólo en los casos en que sea procedente, su eliminación o revocar la autorización otorgada para su tratamiento. Si desea presentar una consulta, reclamo o petición sobre sus datos personales, puede acudir a nuestros canales:

- Correo electrónico idpc.gov.co.atencionciudadania@idpc.gov.co,
- Dirección: Calle 12b # 2 – 96 Bogotá D.C, Colombia.

En el aviso se pueden apreciar los siguientes elementos que lo componen
a) Nombre o razón social y datos de contacto del responsable del tratamiento
b) El Tratamiento al cual serán sometidos los datos y la finalidad del mismo.
c) Los derechos que le asisten al titular.
d) Los mecanismos dispuestos por el responsable para que el titular conozca el manual de política de tratamiento de la información.
e) En todos los casos, debe informar al titular cómo acceder o consultar el manual de política de tratamiento de información.

7. ATENCIÓN DE CONSULTAS Y RECLAMOS

El IDPC cuenta con un procedimiento para la atención de consultas y reclamos por parte de los titulares de los datos personales, así como un área responsable de dicha atención. Además, se establece que la atención de consultas y reclamos debe realizarse de forma oportuna y eficiente, con el objetivo de garantizar el derecho de los titulares de los datos personales a conocer, actualizar, rectificar y revocar su información. Es importante cumplir con estas disposiciones para garantizar el debido proceso y proteger los derechos de los titulares de los datos personales.

El procedimiento está debidamente detallado en el numeral 7. ATENCIÓN DE PETICIONES, CONSULTAS Y RECLAMOS DE DATOS PERSONALES de LA POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES del IDPC https://idpc.gov.co/politica-de-proteccion-de-datos-personales/

8. PROCEDIMIENTO DE GESTION DE ACTIVOS DE INFORMACIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), establece la importancia de mantener un inventario y clasificación de los activos de información[4], por parte de las entidades públicas y privadas que realizan tratamiento de datos personales. Este inventario permite identificar y conocer los diferentes activos de información tratados, lo que facilita la implementación de medidas de seguridad y protección de los datos personales. El MinTIC ha establecido un Modelo de Seguridad y Privacidad de la Información[5], que contempla la elaboración y actualización del inventario de Activos de Información, así como la política de seguridad de la información, para garantizar la protección de los datos personales.

El Instituto Distrital de Patrimonio Cultural, realiza periódicamente el inventarió de activos de información, liderado por el área de Gestión de Sistemas de Información y Tecnología, el registro se realiza en la Matriz de Activos de

[4] https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf
[5] https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

Información, la cual contiene las categorías en donde cada proceso registra sus activos de información que contienen datos personales.
El procedimiento de registro de novedades de datos personales, ante la Superintendencia de Industria y Comercio (SIC), es un proceso importante que permite mantener actualizado el Registro Nacional de Bases de Datos (RNBD)[6]. Las entidades y personas responsables del tratamiento de datos, deben llevar a cabo este procedimiento en la plataforma SIC Facilita, en donde se deberá actualizar la información relacionada con las bases de datos, describiendo las novedades o cambios en los datos personales. Este registro de novedades, es esencial para cumplir con la Ley 1581 de 2012 y garantizar la protección de los datos personales, ya que permite tener una información actualizada y completa de las bases de datos que se están tratando.

9. EVALUACIÓN DE IMPACTO A LA PRIVACIDAD

El Decreto 1377 de 2013 establece la realización de una evaluación de impacto a la privacidad (Privacy Impact Assessment[7], PIA), como una herramienta para identificar los riesgos asociados al tratamiento de datos personales y establecer medidas de mitigación, que permitan garantizar la protección de los derechos de los titulares de los datos. El PIA debe contemplar, entre otros aspectos, la identificación de los datos personales que serán tratados, la finalidad del tratamiento, la identificación de los posibles riesgos asociados al tratamiento de dichos datos y las medidas y mecanismos que se implementarán para mitigar los riesgos identificados. Es importante destacar que la PIA es una herramienta que permite garantizar el cumplimiento de las disposiciones establecidas en el Decreto 1377 de 2013 y evitar posibles sanciones o responsabilidades.

En resumen, la evaluación de impacto a la privacidad es una herramienta esencial para garantizar la protección de los datos personales y cumplir con las disposiciones establecidas en el Decreto 1377 de 2013 12. Su aplicación permite identificar los riesgos asociados al tratamiento de los datos y establecer medidas de mitigación que aseguren la protección de los derechos de los titulares de los datos.

[6] https://www.sic.gov.co/registro-nacional-de-bases-de-datos
[7] Guía sobre el tratamiento de datos personales en entidades estatales www.sic.gov

La validación del análisis de riesgo de ser validado por oficial de protección de datos personales del IDPC.

10. CONTROL DE CAMBIOS

Fecha	**Versión**	**Cambios Introducidos**	**Simplificación o mejora**	**Origen**
29/06/2023	01	Creación del documento.	Mejora	Protección de datos personales – responsabilidad demostrada Decreto 1377 del 2013

11. CRÉDITOS

Elaboró	**Revisó**	**Aprobó**
Ángel Antonio Díaz Vega	Mary Rojas	Aura Herminda López Salazar
Cargo – Rol: Contratista Oficial de Seguridad de la Información Subdirección de Gestión Corporativa	Cargo – Rol: Profesional especializado código 222 grado 03 Subdirección de Gestión Corporativa	Cargo – Rol: subdirectora de la Subdirección de Gestión Corporativa
Documento de aprobación	Memorando interno con N° radicado 20235400088673 del 29-06-2023	