2.

RESOLUCIÓN 20231045

"Por medio del cual se actualiza la versión No. **1** de la Política de Protección de Datos Personales del Instituto para el Desarrollo de Antioquia-IDEA"

El Gerente General del Instituto para el Desarrollo de Antioquia – IDEA – en uso de sus facultades constitucionales y legales, y en especial las conferidas por el artículo 9 y ss. De la Ley 489 de 1998, en la delegación del 19 de diciembre de 2023 de la Junta Directiva del IDEA en la sesión número 21; las conferidas en el numeral 4 y 21 del artículo Décimo sexto de la Resolución de Junta Directiva número 006 del 2014 (Estatutos del Instituto para el Desarrollo de Antioquia – IDEA-) y,

CONSIDERANDO

1. Que la protección de los datos personales está consagrada en el artículo 15 de la Constitución Política como el derecho fundamental que tienen todas las personas a conservar su intimidad personal y familiar y su buen nombre, lo mismo que conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellos en bancos de datos y en archivos de las entidades públicas y privadas. A su vez, el artículo 20 ibidem garantiza a toda persona el derecho fundamental de informar y recibir información veraz e imparcial.

2. Que, en desarrollo de los preceptos constitucionales antes citados, el Congreso de la República expidió la Ley 1266 de 2008, con el objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos personales.

3. Que, a su turno, el artículo 17 de la Ley Estatutaria 1581 de 2012, Régimen General de Protección de Datos Personales consagraron la necesidad de garantizar de forma integral la protección y el ejercicio del derecho fundamental de Hábeas Data y estableció dentro de los deberes de los responsables del tratamiento de datos personales, desarrollar políticas para

este derecho.

4. Que la Ley 1712 de 2014, sobre transparencia y derecho de acceso a la información pública nacional, adiciona nuevos principios, conceptos y procedimientos para el ejercicio y garantía del referido derecho; junto con lo dispuesto en el Libro 2. Parte VIII, Título IV "Gestión de la Información Clasificada y Reservada" del Decreto 1080 de 2015, "por medio del cual se expide el Decreto Reglamentario Único del Sector Cultura", que establece disposiciones sobre el acceso a datos personales en posesión de los sujetos obligados.

5. Que el día 19 de diciembre de 2023, se llevó a cabo la sesión ordinaria No. 21 de Junta Directiva del Instituto para el Desarrollo de Antioquia – IDEA donde se delegó al Gerente General para aprobar la actualización de la Política de tratamiento de Datos Personales de acuerdo con los lineamientos de la Superintendencia de Industria y Comercio, con un plazo máximo hasta el 31 de enero de 2024.

En mérito de lo expuesto, el Gerente General del Instituto para el Desarrollo de Antioquia – IDEA,

RESUELVE:

PRIMERO: **APROBAR LA ACTUALIZACIÓN DE LA POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES DEL INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA,** la cual se anexa al presente acto administrativo y se entiende que hace parte integral del mismo.

SEGUNDO: IMPLEMENTACIÓN, DIFUSIÓN Y SENSIBILIZACIÓN. Ordenar la implementación y difusión a través de los medios institucionales y sensibilización de la Política de Protección de Datos Personales del IDEA, aprobada y adoptada en el artículo anterior.

TERCERO. VIGENCIA. La presente Resolución rige a partir de su publicación y comunicación, de conformidad con lo dispuesto por el artículo 65 de la Ley 1437 de 2011, de manera especial, previa publicación y comunicación a los empleados del IDEA y demás interesados; y deroga todas las disposiciones que le sean contrarias.

CUARTO: **PROCEDENCIA DE RECURSOS.** Contra esta Resolución no procede recurso

alguno, de conformidad con lo establecido con el artículo 75 de la Ley 1437 de 2011.

Dada en Medellín, a los **29-12-2023**

NOTIFÍQUESE, COMUNIQUESE Y CÚMPLASE

JULIÁN SANTIAGO VÁSQUEZ ROLDÁN
Gerente General
Instituto para el Desarrollo de Antioquia -IDEA

Proyectó: SANDRA PATRICIA MENDOZA HINESTROZA
SECRETARIO
DIRECCION DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACION

Aprobó: ANA MARIA GOMEZ CARDONA
GERENTE
GERENCIA DE RIESGOS

Aprobó: ALEXANDER CLAVIJO RAMIREZ
DIRECTOR TÉCNICO
DIRECCION DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACION

Aprobó: JAIR ANTONIO VILLANUEVA RICARDO
GERENTE
GERENCIA DE TI Y OPERACIONES

Aprobó: ISABEL CRISTINA SALAZAR GIRALDO
JEFE DE OFICINA
OFICINA DE PLANEACION ESTRATEGICA

Aprobó: JUAN CARLOS LEDEZMA MATURANA
DIRECTOR TÉCNICO
DIRECCIÓN JURIDICA

Aprobó: LINA MARIA RAMIREZ MURIEL
SECRETARIO GENERAL DE ENTIDAD DESCENTRALIZADA
SECRETARÍA GENERAL

POLÍTICAS DE PROTECCIÓN DE DATOS PERSONALES

Tabla de contenido

1. INTRODUCCIÓN

La Constitución Política de Colombia estableció en el artículo 15 el derecho de protección de datos personales como el derecho de toda persona para conocer, actualizar, rectificar o cancelar la información y datos personales que de ella se hayan recolectado o se traten en bases de datos públicas o privadas.

Mediante la Ley 1581 del 17 de octubre de 2012, el Congreso de la República reglamentó el ya mencionado derecho al establecer las Disposiciones Generales para la Protección de Datos Personales en Colombia, igualmente reglamentada por los Decretos 1377 de 2013 y 886 de 2014 (hoy incorporados en el Decreto único 1074 de 2015), entre otros.

En cumplimiento de las anteriores disposiciones el INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA, consciente de la responsabilidad que les asiste en materia de Tratamiento de Datos Personales de los titulares, ha elaborado la presente POLÍTICA PARA EL TRATAMIENTO DE DATOS PERSONALES, cuya aplicación es de carácter obligatorio para todas las personas naturales o jurídicas que hagan tratamiento de los datos personales registrados en las bases de datos de la Entidad.

El objetivo de esta política es la de proporcionar los lineamientos necesarios para el cumplimiento de las obligaciones legales en materia de protección de datos personales.

2. OBJETIVO

La presente Política tiene como objeto dar la información necesaria y suficiente a los diferentes grupos de interés frente al tratamiento de datos personales, así como establecer los lineamientos que garanticen con ellos el derecho constitucional que tienen todas las personas de conocer, actualizar, rectificar, revocar, suprimir, eliminar la información con datos personales que se hayan recopilado sobre ellas en las bases de datos o archivos del INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA-.

3. ALCANCE

Esta Política aplica a todos los colaboradores del INSTUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA -, y a todas las bases de datos que se encuentren en poder de la entidad donde repose información personal.

Así mismo aplica para las relaciones donde el INSTUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA-, sea el responsable de dicha información y cualquier proveedor o contratista en figura de encargado o custodio de los datos, lo que implica que el proveedor o contratista también debe asegurar el cumplimiento de esta política.

El INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA -IDEA-, dará cumplimiento a las exigencias de la normatividad vigente en materia de Protección de Datos Personales, así como a cualquier exigencia originada en el principio de responsabilidad demostrada y brindará la debida protección a los intereses y necesidades de los titulares de la Información personal tratada por el INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA -.

4. GOBIERNO CORPORATIVO

El INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA -, comprometido con la correcta aplicación y cumplimiento de las normas de Protección de Datos Personales, tendrá al Comité de Ciberseguridad y Seguridad de la Información como instancia de decisión de toda propuesta de modificación, fortalecimiento y mejora de la política para su análisis y aprobación. Adicionalmente, cuenta con otras instancias tales como el Comité de Riesgos y la Junta Directiva, dependiendo de los temas a tratar.

5. NORMATIVIDAD APLICABLE

- ✓ Constitución Política de Colombia
- ✓ Ley 1581 de 2012
- ✓ Decreto 1074 de 2015 Capitulo 25 y Capitulo 26 compilatorios de los decretos:
  - Decreto 1377 de 2013
  - Decreto 886 de 2014
- ✓ Circular 01 del 08 de noviembre 2016

6. GLOSARIO

Las siguientes definiciones se encuentran establecidas en el artículo 3 de la LEPD y artículo 2.2.2.25.1.3 sección 1 Capitulo 25 del decreto 1074 de 2015 (Artículo 3 del decreto 1377 de 2013).

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

Base de Datos: Conjunto organizado de datos personales que sea objeto de tratamiento. Incluye archivos físicos y electrónicos.

Dato Personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Debe entonces entenderse el “dato personal” como una información relacionada con una persona natural (persona individualmente considerada).

Dato Público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o del servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales, sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Dato Semiprivado: Es aquel que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como son: Bases de datos que contengan Información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

Dato Privado: Es un dato personal que por su naturaleza íntima o reservada solo interesa a su titular y para su tratamiento requiere de su autorización previa, informada y expresa. Bases de datos que contengan datos como números telefónicos y correos electrónicos personales; datos laborales, sobre infracciones administrativas o penales, administrados

por administraciones tributarias, entidades financieras y entidades gestoras y servicios comunes de la Seguridad Social, bases de datos sobre solvencia patrimonial o de crédito, bases de datos con información suficiente para evaluar la personalidad del titular, bases de datos de los responsables de operadores que presten servicios de comunicación electrónica.

Dato Sensible: 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 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.

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.

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 de Administrar las Bases de Datos: Colaborador encargado de controlar y coordinar la adecuada aplicación de las políticas del tratamiento de los datos una vez almacenados en una base datos especifica; así como de poner en práctica las directrices que dicte el responsable del tratamiento y el Oficial de Protección de datos.

Oficial de Protección de Datos: Es la persona natural que asume la función de coordinar la implementación del marco legal en protección de datos personales, que dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012.

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

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

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.

Transferencia: La transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un 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 estos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento determinado por el encargado por cuenta del responsable.

7. PRINCIPIOS DE LA PROTECCIÓN DE DATOS

El artículo 4 de la LEPD establece unos principios para el tratamiento de datos personales que se han de aplicar, de manera armónica e integral, en el desarrollo, interpretación y

aplicación de la Ley. Los principios legales de la protección de datos son los siguientes:

Principio de Legalidad: El tratamiento de los datos es una actividad reglada que debe sujetarse a lo establecido en la LEPD, el Decreto 1377 de 2013 Compilado en el Capítulo 25 del Decreto 1074 de 2015 y en las demás disposiciones que la desarrollen.

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 Libertad: El tratamiento solo puede ejercerse con el consentimiento previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que revele el consentimiento. El tratamiento de los datos requiere la autorización previa e informada del Titular por cualquier medio que permita ser consultado con posterioridad.

Principio de veracidad o Calidad: La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

Principio de Transparencia: En el tratamiento debe garantizarse el derecho del titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan. En el momento de solicitar la autorización al titular, el responsable del tratamiento deberá informarle de manera clara y expresa lo siguiente, conservando prueba del cumplimiento de este deber:

- ✓ El tratamiento al cual será sometidos sus datos y la finalidad de este.
- ✓ El carácter facultativo de la respuesta del Titular a las preguntas que le sean hechas cuando éstas traten sobre datos sensibles o sobre datos de niños, niñas o adolescentes.
- ✓ Los derechos que le asisten como Titular.
- ✓ La identificación, dirección física, correo electrónico y teléfono del responsable del tratamiento.

Principio de acceso y circulación Restringida: El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la LEPD y la Constitución. En este sentido, el tratamiento solo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la Ley. Los datos personales, salvo la información pública, no podrán estar disponibles en Internet y otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los titulares o terceros autorizados conforme a la Ley.

Principio de Seguridad: La información sujeta a tratamiento por el responsable del tratamiento o encargado del tratamiento se deberá manejar con 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. El responsable del tratamiento tiene la responsabilidad de implantar las medidas de seguridad correspondientes y de ponerlas en conocimiento de todo el personal que tenga acceso, directo o indirecto, a los datos.

Principio de confidencialidad: Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos 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 solo realizar suministro o comunicación

de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la LEPD y en los términos de esta.

8. AUTORIZACIÓN DE LA POLÍTICA DE TRATAMIENTO

De acuerdo con el artículo 9 de la LEPD, para el tratamiento de datos personales se requiere la autorización previa e informada del Titular. Mediante la aceptación de la política, todo Titular que facilite información relativa a sus datos personales está consintiendo el tratamiento de sus datos por parte de INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA -IDEA-, en los términos y condiciones recogidos en la misma.

No será necesaria la autorización del Titular cuando se trate de:

- ✓ 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.
- ✓ Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- ✓ Datos relacionados con el Registro Civil de las personas.

El Instituto tendrá a disposición de los terceros el aviso de tratamiento de datos.

9. RESPONSABLE DEL TRATAMIENTO

El responsable del tratamiento de las bases de datos objeto de esta política es el INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA -, cuyos datos de contacto son los siguientes:

Dirección: CL 42 #52-259, MEDELLÍN, ANTIOQUIA
Correo electrónico: protecciondatos@idea.gov.co
Teléfono: 3547700

10. TRATAMIENTO Y FINALIDADES DE LAS BASES DE DATOS

El INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA -, en el desarrollo de su actividad empresarial, lleva a cabo el tratamiento de datos personales que están contenidos y son tratados en bases de datos destinadas a finalidades legítimas, cumpliendo con la Constitución y la Ley.

El Anexo 1 PL-01 denominado Organización Bases de Datos, contiene la información relativa a las distintas bases de datos responsabilidad de la empresa y las finalidades asignadas a cada una de ellas para su tratamiento.

11. DERECHOS DE LOS TITULARES

De acuerdo con el artículo 8 de la LEPD, articulo 2.2.2.25.4.1 sección 4 capítulo 25 del Decreto 1074 de 2015 (Artículos 21 y 22 del Decreto 1377 de 2013), los titulares de los

datos pueden ejercer una serie de derechos en relación con el tratamiento de sus datos personales. Estos derechos podrán ejercerse por las siguientes personas.

- ✓ A los Titulares, sus causahabientes o sus representantes legales.
- ✓ A las Entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.
- ✓ A los terceros autorizados por el Titular o por la ley.

Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.

Los derechos del Titular son los siguientes:

Derecho de acceso o consulta: Se trata del derecho del Titular a ser informado por el responsable del tratamiento, previa solicitud, respecto al origen, uso y finalidad que les han dado a sus datos personales.

Derechos de quejas y reclamos: La Ley distingue cuatro tipos de reclamos:

- ✓ *Reclamo de corrección:* Es el derecho del Titular a que se actualicen, rectifiquen o modifiquen aquellos datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
- ✓ *Reclamo de supresión*: Es el derecho del Titular a que se supriman los datos que resulten inadecuados, excesivos o que no respeten los principios, derechos y garantías constitucionales y legales.
- ✓ *Reclamo de revocación:* Es el derecho del Titular a dejar sin efecto la autorización previamente prestada para el tratamiento de sus datos personales.
- ✓ *Reclamo de infracción*: Es el derecho del Titular a solicitar que se subsane el incumplimiento de la normativa en materia de Protección de Datos.

Derecho a solicitar prueba de la autorización otorgada al responsable del tratamiento: Salvo cuando expresamente se exceptúe como requisito para el tratamiento de conformidad con lo previsto en el artículo 10 de la LEPD.

Derecho a presentar ante la Superintendencia de Industria y Comercio quejas por infracciones: El titular o causahabiente solo podrá elevar ante la SIC – Superintendencia de Industria y Comercio la petición (queja), una vez haya agotado el trámite de consulta o reclamo ante el responsable del tratamiento o encargado del tratamiento.

12. SOLICITUD DE AUTORIZACIÓN AL TITULAR DEL DATO PERSONAL

Con antelación o al momento de efectuar la recolección del dato personal, el INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA -, solicitará al titular del dato su autorización para efectuar su recolección y tratamiento, indicando la finalidad para la cual se solicita el dato, utilizando para esos efectos medios técnicos automatizados, escritos u orales, que permitan conservar prueba de la autorización o de la conducta inequívoca descrita en el artículo 2.2.2.25.2.2. sección 2 del capítulo 25 del Decreto 1074 de 2015 (Artículo 7 del Decreto 1377 de 2013).

13. TRATAMIENTO DE DATOS DE MENORES

De acuerdo con el artículo 7° de la Ley 1581 de 2012, el tratamiento de datos personales de niños, niñas y adolescentes está prohibido, salvo lo dispuesto en el artículo 2.2.2.25.2.9 sección 2 del capítulo 25 del Decreto 1074 de 2015 (Artículo 12 del Decreto 1377 de 2013) y en cumplimiento de los siguientes parámetros y requisitos:

- ✓ Que responda y respete el interés superior de los niños, niñas y adolescentes.
- ✓ Que se asegure el respeto de sus derechos fundamentales.

Cumplidos los anteriores requisitos, el INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA -, solicitará al representante legal del niño, niña o adolescente la autorización 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.

El responsable y encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos, aplicando los principios y obligaciones establecidos en la Ley 1581 de 2012 y normas reglamentarias.

14. ATENCIÓN A LOS TITULARES DE DATOS

El Oficial de Protección de Datos del INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA - IDEA - será el encargado de asegurar la atención de peticiones, consultas y reclamos ante la cual el titular de los datos puede ejercer sus derechos. Teléfono: 3547700. Correo electrónico: protecciondatos@idea.gov.co.

15. PROCEDIMIENTOS PARA EJERCER LOS DERECHOS DEL TITULAR

15.1. Derecho de acceso o consulta

Según el artículo 2.2.2.25.4.2. sección 4 capítulo 25 del Decreto 1074 de 2015 (Artículo 21 del Decreto 1377 de 2013), el titular podrá consultar de forma gratuita sus datos personales en dos casos:

- ✓ Al menos una vez cada mes calendario.
- ✓ Cada vez que existan modificaciones sustanciales de las políticas de tratamiento de la información que motiven nuevas consultas.

Para consultas cuya periodicidad sea mayor a una por cada mes calendario, el INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA - IDEA -, solamente podrá cobrar al titular gastos de envío, reproducción y, en su caso, certificación de documentos.

Los costos de reproducción no podrán ser mayores a los costos de recuperación del material correspondiente. Para tal efecto, el INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA - demostrará a la Superintendencia de Industria y Comercio, cuando ésta así lo requiera, el soporte de dichos gastos.

El titular de los datos puede ejercer el derecho de acceso o consulta de sus datos mediante correo postal o electrónico dirigido al INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA - indicando el derecho que quiere ejercer. Si es correo postal debe

ser remitido a la CL 42 #52-259, MEDELLÍN, ANTIOQUIA. Si la solicitud es por correo electrónico, éste debe ser dirigido a protecciondatos@idea.gov.co.

La solicitud deberá contener los siguientes datos:

- ✓ Nombre y apellidos del Titular.
- ✓ Número de la Cédula de Ciudadanía del Titular y, acorde al caso, adicional el número de cédula de la persona que lo representa, así como del documento acreditativo de tal representación.
- ✓ Petición en que se concreta la solicitud de acceso o consulta.
- ✓ Dirección para notificaciones, fecha y firma del solicitante.
- ✓ Documentos acreditativos de la petición formulada, cuando corresponda.

Una vez recibida la solicitud, el INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA - resolverá la petición de consulta en un plazo máximo de diez (10) días hábiles contados a partir de la fecha de recibo de esta.

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. Estos plazos están fijados en el artículo 14 de la LEPD.

Una vez agotado el trámite de consulta, el titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

15.2. Derechos de quejas y reclamos

El titular de los datos puede ejercitar los derechos de reclamo sobre sus datos mediante un escrito dirigido al INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA - mediante correo electrónico a protecciondatos@idea.gov.co o a través de correo postal remitido a CL 42 #52-259, MEDELLÍN, ANTIOQUIA.

La solicitud deberá contener los siguientes datos:

- ✓ Nombre y apellidos del Titular.
- ✓ Número de la Cédula de Ciudadanía del Titular y, acorde al caso, adicional el número de cédula de la persona que lo representa, así como del documento acreditativo de tal representación.
- ✓ Descripción de los hechos y petición en que se concreta la solicitud de corrección, supresión, revocación o infracción.
- ✓ Dirección para notificaciones, fecha y firma del solicitante.
- ✓ Documentos acreditativos de la petición formulada que se quieran hacer valer, cuando corresponda.

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.

Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga “reclamo en trámite” y el motivo de este, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

El INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA - resolverá la petición de consulta en un plazo máximo de quince (15) días hábiles contados a partir de la fecha de recibo de esta.

Cuando no fuere posible atender al 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.

Una vez agotado el trámite de reclamo, el titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

16. ACCIONES GENERALES PARA LA PROTECCIÓN DE DATOS PERSONALES

A continuación, se establecen los lineamientos generales aplicados por El INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA -, con el fin de cumplir con sus obligaciones en cumplimiento de los principios para la administración de datos personales. Estos lineamientos son complementarios a las políticas, procedimientos o instructivos generales actualmente existentes e implementados.

16.1. Tratamiento de la Información

Todos los miembros de la Entidad, al realizar las actividades propias de su cargo, asumirán las responsabilidades y las obligaciones que se tienen en el manejo adecuado de la información personal, desde su recolección, almacenamiento, uso, circulación y hasta su disposición final.

16.2. Uso de la Información

La información de carácter personal contenida en las bases de datos debe ser utilizada y tratada de acuerdo con las finalidades descritas en el archivo “Anexo 1 PL-01. Organización Bases de Datos”.

En caso de que algún área identifique nuevos usos diferentes a los descritos en la presente política de tratamiento de datos personales, deberá informar al Oficial de Protección de Datos Personales, quien evaluará y gestionará, cuando aplique, su inclusión en la presente política.

Igualmente, se deben tomar en consideración los siguientes supuestos:

- ✓ En caso de que un área diferente de la que recolectó inicialmente el dato personal requiera utilizar los datos personales que se han obtenido, ello se podrá hacer siempre que se trate de un uso previsible por el tipo de servicios que ofrece la Entidad y para una finalidad contemplada dentro de la presente Política de Tratamiento de Datos Personales.
- ✓ Cada área debe garantizar que en las prácticas de reciclaje de documentos físicos no se divulgue información confidencial ni datos personales. Por lo anterior, no se podrán reciclar hojas de vida, ni títulos académicos, ni certificaciones académicas o

laborales, ni resultados de exámenes médicos ni ningún documento que contenga información que permita identificar a una persona.

- ✓ En caso de que un encargado haya facilitado datos personales o bases de datos a algún área para un fin determinado, el área que solicitó los datos personales no debe utilizar dicha información para una finalidad diferente de la relacionada en la Política de Tratamiento de Datos Personales; al finalizar la actividad, es deber del área que solicitó la información, eliminar la base de datos o los datos personales utilizados evitando el riesgo de desactualización de información o casos en los cuales durante ese tiempo un titular haya presentado algún reclamo.
- ✓ Únicamente los funcionarios y contratistas autorizados pueden introducir, modificar o anular los datos contenidos en las bases de datos o documentos objeto de protección. Los permisos de acceso de los usuarios son concedidos por la Gerencia de TI y Operaciones, de acuerdo con los perfiles establecidos, los cuales serán previamente definidos por los líderes de los procesos donde se requiera el uso de información personal.
- ✓ Cualquier uso de la información diferente al establecido, será previamente consultado con el Oficial de Protección de Datos Personales.

16.3. Almacenamiento de la Información

El almacenamiento de la información digital y física se realiza en medios o ambientes que cuentan con adecuados controles para la protección de los datos. Esto involucra controles de seguridad física e informática, tecnológicos y de tipo ambiental en áreas restringidas, en instalaciones propias y/o centros de cómputo o centros documentales gestionados por terceros.

16.4. Destrucción

La destrucción de la información personal ya sea en medios físicos o electrónicos se realiza a través de mecanismos que no permiten su reconstrucción. Se realiza únicamente en los casos en que no constituya el desconocimiento de norma legal alguna, dejando siempre la respectiva trazabilidad de la acción. La destrucción comprende información contenida en poder de terceros como en instalaciones propias.

17. GESTIÓN DE INCIDENTES CON DATOS PERSONALES

Se entiende por incidencia cualquier anomalía que afecte o pudiera afectar la seguridad de las bases de datos o información contenida en las mismas. En caso de conocer alguna incidencia ocurrida, el usuario debe comunicarla al Oficial de Protección de Datos que adoptará las medidas oportunas frente al incidente reportado. El Oficial de Protección de Datos Personales informará de la incidencia a la Delegatura de Protección de Datos Personales de LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO, en el módulo habilitado para tal efecto dentro de los 15 días a partir del conocimiento de esta

Las incidencias pueden afectar tanto a bases de datos digitales como físicas y generarán las siguientes actividades:

Notificación de Incidentes: Cuando se presuma que un incidente pueda afectar o haber

afectado a bases de datos con información personal datos personales se deberá informar al Oficial de Protección de Datos Personales quién gestionará su reporte en el Registro Nacional de Bases de Datos.

Gestión de Incidentes: Es responsabilidad de cada funcionario, contratista, consultor o tercero, reportar de manera oportuna cualquier evento sospechoso, debilidad o violación de políticas que pueden afectar la confidencialidad, integridad y disponibilidad de los activos e información personal de la Entidad.

Identificación: Todos los eventos sospechosos o anormales, tales como aquellos en los que se observe el potencial de perdida de reserva o confidencialidad de la información, deben ser evaluados para determinar si son o no, un incidente y deben ser reportados al nivel adecuado en la organización. Cualquier decisión que involucre a las autoridades de investigación y judiciales debe ser hecha en conjunto entre el Oficial de Protección de Datos Personales y la Dirección Jurídica.

Reporte: Todos los incidentes y eventos sospechosos deben ser reportados tan pronto como sea posible a través de los canales internos establecidos por el INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA -.

Si la información sensible o confidencial es perdida, divulgada a personal no autorizado o se sospecha de alguno de estos eventos, el Oficial de Protección de Datos Personales, debe ser notificado de forma inmediata. Los funcionarios deben reportar a su jefe directo y al Oficial de Protección de Datos Personales cualquier daño o pérdida de computadores o cualquiera otro dispositivo, cuando estos contengan datos personales en poder de la Entidad. A menos que exista una solicitud de la autoridad competente debidamente razonada y justificada, ningún funcionario debe divulgar información sobre sistemas de cómputo, y redes que hayan sido afectadas por un delito informático o abuso de sistema. Para la entrega de información o datos en virtud de orden de autoridad, la Dirección Jurídica deberá intervenir con el fin de prestar el asesoramiento adecuado.

Contención, Investigación y Diagnostico: El Oficial de Protección de Datos Personales debe garantizar que se tomen acciones para investigar y diagnosticar las causas que generaron el incidente, así como también debe garantizar que todo el proceso de gestión del incidente sea debidamente documentado, apoyado por la Gerencia de TI y Operaciones.

En caso de que se identifique un delito informático, en los términos establecidos en la Ley 1273 de 2009, el Oficial de Protección de Datos Personales y la Dirección Jurídica, reportará tal información a las autoridades de investigaciones judiciales respectivas. Durante los procesos de investigación se deberá garantizar la “Cadena de Custodia” con el fin de preservarla en caso de requerirse establecer una acción legal.

Solución: La Gerencia de TI y Operaciones así como cualquier área comprometida y los directamente responsables de la gestión de datos personales, deben prevenir que el incidente de seguridad se vuelva a presentar, corrigiendo todas las vulnerabilidades existentes.

Cierre de Incidente y Seguimiento: El Oficial de Protección de Datos Personales y las áreas que usan o requieren la información, iniciarán y documentarán todas las tareas de

revisión de las acciones que fueron ejecutadas para remediar el incidente de seguridad. El Oficial de Protección de Datos Personales preparará un análisis anual de los incidentes reportados. Las conclusiones de este informe se utilizarán en la elaboración de campañas de concientización que ayuden a minimizar la probabilidad de incidentes futuros.

Reporte de incidentes ante la SIC como autoridad de control: Se reportarán como novedades los incidentes de seguridad que afecten la base de datos, dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos. Los líderes de proceso y/o propietarios de activos de información, reportarán de forma interna los incidentes asociados a datos personales ante el Oficial de Protección de Datos Personales, quién dentro del plazo legal procederá a reportarlos ante el Registro Nacional de Bases de Datos.

18. CONTROL DE ACCESO Y VIDEO VIGILANCIA

Control Acceso

Las áreas donde se ejecutan procesos relacionados con información confidencial o restringida deben contar con controles de acceso que sólo permitan el ingreso a los colaboradores autorizados y que permita guardar la trazabilidad de los ingresos y salidas.

Video Vigilancia

La Entidad cuenta con cámaras de video vigilancia, cumpliendo con los parámetros establecidos en la Guía para la Protección de Datos Personales en Sistemas de Videovigilancia, expedidos por la SIC como autoridad de control.

Las imágenes deberán ser conservadas por un tiempo máximo de 90 días.

En caso de que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

19. CAPACITACIÓN DE FUNCIONARIOS Y CONTRATISTAS

El INSTITUTO PARA EL DESARROLLO DE ANQUIOQUIA – IDEA -, desarrollará programas anuales de capacitación y concientización en Protección de datos personales.

La Entidad debe poner en conocimiento estas políticas por el medio que considere adecuado y con ello, capacitar a sus funcionarios y contratistas en la administración de los datos personales con una periodicidad al menos anual, con el fin de medir sus conocimientos sobre el particular.

Los nuevos funcionarios y contratistas, al momento de vincularse con la Entidad, deben recibir capacitación sobre Protección de datos personales dejando constancia de su asistencia y conocimiento.

En el desarrollo de los programas de capacitación y concientización se deberá asegurar que los funcionarios, contratistas y terceros conozcan sus responsabilidades.

20. PROCESOS DE REVISIÓN Y AUDITORÍAS DE CONTROL

La Entidad realizará procesos de revisión o auditorías en materia de protección de datos personales verificando de manera directa o a través de terceros, que las políticas y procedimientos se han implementado adecuadamente en la Entidad. Con base a los resultados obtenidos, se diseñarán e implementarán los planes de mejoramiento (preventivos, correctivos y de mejora) necesarios.

Por regla general el INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA - realizará estos procesos de revisión con una periodicidad mínima de un año o de forma extraordinaria ante incidentes graves que afecten a la integridad de las bases de datos personales. Los resultados de la revisión junto con los eventuales planes de mejoramiento serán presentados por el Oficial de Protección de Datos Personales al comité de Ciberseguridad y Seguridad de la Información para su valoración y aprobación.

21. ADMINISTRACIÓN DE RIESGOS

El INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA - ha identificado riesgos relacionados con el tratamiento de los datos personales y establecido controles con el fin de mitigar sus causas.

Por ello, establecerá un sistema de gestión de riesgos junto con las herramientas, indicadores y recursos necesarios para su administración.

El sistema de gestión de riesgos determinará las fuentes tales como: tecnología, recurso humano, infraestructura y procesos que requieren protección, sus vulnerabilidades y las amenazas, con el fin de valorar su nivel de riesgo. Por lo que, para garantizar la protección de datos personales se tendrá en cuenta el tipo o grupo de personas internas y externas, los diferentes niveles de autorización de acceso. Asimismo, se observará la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial), tales como:

Criminalidad: Entendida como las acciones, causadas por la intervención humana, que violan la ley y que están penalizadas por ésta.

Sucesos de origen físico: Entendidos como los eventos naturales y técnicos, así como, los eventos indirectamente causados por la intervención humana.

Negligencia y decisiones institucionales: Entendidos como las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema. Al mismo tiempo son las amenazas menos predecibles porque están directamente relacionado con el comportamiento humano.

El INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA - en el sistema de gestión de riesgo implementará las medidas de protección para evitar o minimizar los daños en caso de que se materialice una amenaza.

La documentación relacionada con el sistema de administración de este tipo de riesgos estará a cargo de la Dirección de Ciberseguridad y Seguridad de la Información, para lo que puede hacer uso de herramientas tecnológicas, si lo considera necesario.

22. TRANSFERENCIA DE DATOS A TERCEROS PAÍSES

De acuerdo con el Título VIII de la LEPD, se prohíbe la transferencia de datos personales a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios. Esta prohibición no regirá cuando se trate de:

- ✓ 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.

Se debe tener en cuenta que, en los casos no contemplados como excepción, corresponderá a la Superintendencia de Industria y Comercio proferir la declaración de conformidad relativa a la transferencia internacional de datos personales.

Las transmisiones internacionales de datos personales que se efectúen entre el INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA - y un encargado para permitir que el encargado realice el tratamiento por cuenta del responsable, no requerirán ser informadas al titular ni contar con su consentimiento, siempre que exista un contrato de transmisión de datos personales.

23. TRATAMIENTO DE DATOS BIOMÉTRICOS

Los datos biométricos almacenados en las bases de datos son recolectados y tratados por motivos estrictamente de seguridad, para verificar la identidad personal y realizar control de acceso a los empleados, clientes y visitantes. Los mecanismos biométricos de identificación capturan, procesan y almacenan información relacionada con, entre otros, los rasgos físicos de las personas (las huellas dactilares, reconocimiento de voz y los aspectos faciales), para poder establecer o “autenticar” la identidad de cada sujeto.

La administración de las bases de datos biométrica se debe ejecutar con medidas de seguridad técnicas que garantizan el debido cumplimiento de los principios y las obligaciones derivadas de Ley Estatutaria en Protección de Datos asegurando además la confidencialidad y reserva de la información de los titulares.

24. REGISTRO NACIONAL DE BASES DE DATOS - RNBD

El término para registrar las bases de datos en el RNBD será el establecido legalmente.

Asimismo, de acuerdo con el artículo 12 del Decreto 886 de 2014, los responsables del tratamiento deberán inscribir sus bases de datos en el Registro Nacional de Bases de Datos en la fecha en que la Superintendencia de Industria y Comercio habilite dicho registro, de acuerdo con las instrucciones que para el efecto imparta esa entidad. Las bases de Datos que se creen con posterioridad a ese plazo deberán inscribirse dentro de los dos (2) meses siguientes, contados a partir de su creación.

25. SEGURIDAD DE LA INFORMACIÓN Y DATOS PERSONALES

El cumplimiento del marco normativo en Protección de Datos Personales, la seguridad, reserva y/o confidencialidad de la información almacenada en las bases de datos es de vital importancia para el INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA -IDEA-. Por ello, hemos establecido políticas, lineamientos, procedimientos y estándares de seguridad de la información, los cuales podrán cambiar en cualquier momento ajustándose a nuevas normas y necesidades del INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA -IDEA- cuyo objetivo es proteger y preservar la integridad, confidencialidad y disponibilidad de la información y datos personales.

Asimismo, el INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA – IDEA – garantizará que, en la recolección, almacenamiento, uso, tratamiento, destrucción o eliminación de la información suministrada, se realizará cumpliendo la regulación y políticas establecidas para tal fin.

26. GESTIÓN DE DOCUMENTOS

Los documentos que contengan datos personales deben ser fácilmente recuperables, es por ello que se debe dejar documentado el lugar donde reposa cada uno de los documentos tanto físicos como digitales, se deben hacer inspecciones a estas rutas de almacenamiento de forma frecuente, se debe garantizar su conservación dejando definido en que soporte y bajo qué condiciones se llevará a cabo esta conservación, teniendo en cuenta condiciones ambientales, lugares de almacenamiento, riesgos a los cuales están expuestos entre otros, el tiempo de retención de los documentos se determina en función de los requisitos legales si aplica, de lo contrario cada organización lo define de acuerdo a sus necesidades, así mismo debe tener clara la disposición final de los mismos, identificando si se recicla, reutiliza, se conserva, se digitaliza entre otros.

Los documentos que tienen que ver con la protección de datos personales deben ser elaborados por personal o una entidad competente para ello, así mismo la organización debe ser quien revise y apruebe todos los documentos y lo deje registrado en la casilla de aprobación de los documentos.

A fin de que sean fácilmente trazables, los documentos deberán estar codificados, serán actualizados y modificados por el personal responsable, esta modificación se efectuara siempre y cuando sea necesario, para la eliminación de un documento se debe tener la justificación para ello descrita en el histórico el cual se encuentra en la parte inferior de todos los documentos.

La distribución de los documentos que contengan datos personales la efectuará el responsable del tratamiento, este dejará documentada la evidencia de dicha distribución, donde entre otros se especifique; el tipo de documento y la identificación de la persona a

la cual se le entregó la información se deberá designar un responsable de garantizar la confidencialidad de los datos personales de los titulares, este será quien custodie documentos, garantice su protección tanto física como digital, evite alteraciones de la información, así mismo garantizará que los documentos que salgan de su custodia sean identificados y fácilmente trazables.