

CONCEPTO 62686 DE 2020

(diciembre 15)

<Fuente: Archivo interno entidad emisora>

SERVICIO NACIONAL DE APRENDIZAJE - SENA

PARA: XXXXXXXXX Coordinadora Nacional de Servicio al Ciudadano - Dirección General – 1-8086
DE: Coordinador Grupo de Conceptos Jurídicos y Producción Normativa 1-0014
ASUNTO: Concepto tratamiento de datos personales recolectados por canales oficiales del SENA – adopción de protocolos y mecanismos de seguridad

En atención a la solicitud formulada mediante correo electrónico sin radicar de fecha 7 de diciembre de 2020 en el cual consulta sobre cómo se puede proceder con respecto al tratamiento de datos personales de información recopilada de los ciudadanos que se acercan a la entidad a través de los canales oficiales establecidos para tal fin (presencial, telefónico y virtual); al respecto, de manera comedida respondo la solicitud, teniendo en cuenta los siguientes antecedentes:

Informa que para la medición de la satisfacción por la atención realizada a los ciudadanos a través de los diferentes canales, en especial sobre el canal presencial, se envía una encuesta a las personas que fueron registradas en el formulario de Google. En la encuesta se hace la solicitud de autorización de datos personales - Habeas Data, la cual contiene un texto en el que se destaca: “(...) En este sentido, el SENA queda autorizado de manera expresa e inequívoca para mantener y manejar toda mi información personal y profesional para los fines que se encuentra legal y reglamentariamente facultado.

Sin perjuicio de lo anterior, los referidos datos no podrán ser distribuidos, comercializados, compartidos, suministrados o intercambiados con terceros, y en general, realizar actividades en las cuales se vea comprometida la confidencialidad y protección de la información recolectada, y podré en cualquier momento solicitar que la información sea modificada, actualizada o retirada de las bases de datos del SENA...”.

En la consulta formulada puntualiza:

“(...) una de las preguntas de la encuesta de medición de la satisfacción del canal presencial es la siguiente:

“¿Usted acudió a algún tramitador, para gestionar el servicio o el trámite por el que acudió a la entidad? *

*Entiéndase como "Tramitador" a cualquier persona externa / interna al SENA que le ayudó con su solicitud y le cobró dinero por el servicio o trámite.”

Teniendo en cuenta que algunas personas han respondido afirmativamente a la pregunta mencionada, esta Coordinación remitió los resultados a los Despachos Regionales y Centros de Formación Profesional correspondientes, para que se tomen medidas preventivas y si es el caso correctivas frente a la situación que se presenta.

Por lo anterior, se han recibido solicitudes de algunas dependencias para que se les comparta la

información de las personas que respondieron afirmativamente a la pregunta relacionada con los “tramitadores”, con el ánimo de contactarlas para poder tener información más precisa sobre la respuesta dada”.

De acuerdo con lo anterior formula unos interrogantes, los cuales serán respondidos más adelante.

ALCANCE DE LOS CONCEPTOS JURÍDICOS

Los conceptos emitidos por la Dirección Jurídica del SENA son orientaciones de carácter general que no comprenden la solución directa de problemas específicos ni el análisis de actuaciones particulares. En cuanto a su alcance, no son de obligatorio cumplimiento o ejecución, ni tienen el carácter de fuente normativa y sólo pueden ser utilizados para facilitar la interpretación y aplicación de las normas jurídicas vigentes.

PRECEDENTES NORMATIVOS

Para el análisis del presente concepto se tendrán en cuenta los siguientes fundamentos normativos:

Constitución Política de 1991 artículo [15](#)

Ley [1581](#) de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”.

Decreto [1081](#) de 2015 “Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República”

Acuerdo [013](#) de 2019, expedido por el Consejo Directivo Nacional, por el cual se aprobó la Política General de Seguridad de la Información y Protección de Datos Personales en el SENA y se adoptó el Manual de la Política General de Seguridad de la Información y Protección de Datos Personales del SENA.

Resolución [359](#) de 2016 “Por la cual se reglamenta el trámite de las peticiones y la atención de quejas, reclamos y sugerencias en el Servicio Nacional de Aprendizaje (Sena), se asignan unas funciones y se deroga la Resolución número [725](#) de 2013”. Modificada por la Resolución [2259](#) de 2017, por la cual se reglamenta el trámite de las peticiones verbales.

ANÁLISIS JURÍDICO

1º El artículo [15](#) de la Constitución Política fija el contenido tanto del derecho a la intimidad como a la protección de los datos personales:

“ARTÍCULO [15](#). Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que

establezca la ley.

Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley”.

2°. Por medio de la Ley [1581](#) de 2012 se expidió el marco general de la protección de los datos personales en Colombia, cuyo artículo [2](#) establece que los principios y disposiciones en ella contenidos “serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales”.

El artículo [4](#) ibidem consagra los principios para el tratamiento de datos personales, indicando:

“Artículo [4](#). Principios para el Tratamiento de datos personales. En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:

- a) Principio de legalidad en materia de Tratamiento de datos: El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen;
- b) 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;
- c) Principio de libertad: El Tratamiento sólo 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 releve el consentimiento;
- d) 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;
- e) 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;
- f) 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 presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley;

Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley;

- g) Principio de seguridad: La información sujeta a Tratamiento por el Responsable del

Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, 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;

h) 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 sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma”.

El artículo [9](#) ut supra determina que, sin perjuicio de las excepciones previstas en dicha ley, “en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior”. (Negrilla y subrayado fuera de texto)

Conforme con el artículo [10](#) de la Ley 1581 de 2012 no se requiere la autorización del titular para la entrega de cierta información personal:

“Artículo [10](#). Casos en que no es necesaria la autorización. La autorización del Titular no será necesaria cuando se trate de:

- a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;
- b) Datos de naturaleza pública;
- c) Casos de urgencia médica o sanitaria;
- d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;
- e) Datos relacionados con el Registro Civil de las Personas.

Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley”.

En relación con el uso de “datos sensibles”, el artículo [5](#) de dicha norma establece:

“ARTÍCULO [5o](#). DATOS SENSIBLES. Para los propósitos de la presente ley, 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” (Negrilla fuera de texto)

Frente al tratamiento que debe darse a los datos sensibles, el artículo [6](#) de la norma ut supra prevé:

“ARTÍCULO [6o](#). TRATAMIENTO DE DATOS SENSIBLES. Se prohíbe el Tratamiento de datos sensibles, excepto cuando:

El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;

b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización;

c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular;

d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;

e) El Tratamiento tenga una finalidad histórica, estadística o científica.

En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares”.

En cuanto al derecho a solicitar la información respecto de datos personales consignada en una entidad, el artículo [13](#) de la Ley 1581 de 2012 prevé que las personas a quienes es posible suministrar la información son:

(i) los Titulares, sus causahabientes o sus representantes legales; (ii) las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial; y (iii) los terceros autorizados por el Titular o por la ley.

3°. El Decreto [1081](#) de 2015 “Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República” establece:

“ARTÍCULO [2.1.1.4.1](#). Excepciones al Derecho fundamental de acceso a la información pública. Los sujetos obligados garantizarán la eficacia del ejercicio del derecho fundamental de acceso a la información pública, sin perjuicio de su facultad de restringirlo en los casos autorizados por la Constitución o la ley, y conforme a lo previsto en los artículos [18](#) y [19](#) la Ley 1712 de 2014, en consonancia con las definiciones previstas en los literales c) y d) del artículo [6](#), de la misma.

“ARTÍCULO [2.1.1.4.1.1](#). Acceso general a datos semiprivados, privados o sensibles. La información pública que contiene datos semiprivados o privados, definidos en los literales g) y h) del artículo [3](#) de la Ley 1266 de 2008, o datos personales o sensibles, según lo previsto en los artículos [3](#) y [5](#) de la Ley 1581 de 2012 y en el numeral 3 del artículo 3 del Decreto 1377 de 2013, solo podrá divulgarse según las reglas establecidas en dichas normas.

“ARTÍCULO 2.1.1.4.1.2. Acceso a datos personales en posesión de los sujetos obligados. Los sujetos obligados no podrán permitir el acceso a datos personales sin autorización del titular de la información, salvo que concurra alguna de las excepciones consagradas en los artículos [6](#) y [10](#) de la Ley 1581 de 2012.

Tampoco podrá permitirse el acceso a los datos personales de niños, niñas y adolescentes, salvo aquellos que sean de naturaleza pública, de acuerdo con lo previsto en el artículo [7](#) de la Ley

1581 de 2012.

PARÁGRAFO 1. Permitir el acceso de un dato semiprivado, privado o sensible no le quita el carácter de información clasificada, ni puede implicar su desprotección.

PARÁGRAFO 2. Salvo que medie autorización del titular, a los datos semiprivados, privados y sensibles contenidos en documentos públicos solo podrá accederse por decisión de autoridad jurisdiccional o de autoridad pública o administrativa competente en ejercicio de sus funciones”.

4°. Acorde con lo previsto en las leyes estatutarias enunciadas, en el SENA se expidió la Resolución [359](#) de 2016, la cual tiene por objeto regular el trámite interno de las peticiones que se formulen ante el Servicio Nacional de Aprendizaje (Sena) a nivel nacional conforme con la estructura y organización contenida en el Decreto [0249](#) de 2004 y las normas que lo modifiquen y adicionen. Dicha resolución, en torno a los documentos e información reservada y a datos privados, semiprivados y sensibles, establece:

“ARTÍCULO [30](#). ACCESO A DATOS PERSONALES EN POSESIÓN DE LOS SUJETOS OBLIGADOS. Los sujetos obligados no podrán permitir el acceso a datos personales sin autorización del titular de la información, salvo que concurra alguna de las excepciones consagradas en los artículos [60](#) y [10](#) de la Ley 1581 de 2012 que se citan a continuación:

Tratamiento de datos sensibles. Se prohíbe el tratamiento de datos sensibles, excepto cuando:

- a) El Titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;
- b) El tratamiento sea necesario para salvaguardar el interés vital del titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización;
- c) El tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del titular;
- d) El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;
- e) El tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los titulares.

Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la Ley [1581](#) de 2012.

Tampoco podrá permitirse el acceso a los datos personales de niños, niñas y adolescentes, salvo aquellos que sean de naturaleza pública, de acuerdo con lo previsto en el artículo [70](#) de la Ley 1581 de 2012.

PARÁGRAFO 1o. Permitir el acceso de un dato semiprivado, privado o sensible no le quita el carácter de información clasificada, ni puede implicar su desprotección.

PARÁGRAFO 2o. Salvo que medie autorización del titular, a los datos semiprivados, privados y sensibles contenidos en documentos públicos solo podrá accederse por decisión de autoridad jurisdiccional o de autoridad pública o administrativa competente en ejercicio de sus funciones. (Decreto número 103 de 2015, artículo [26](#)).

“ARTÍCULO [31](#). AUTORIZACIÓN DEL TITULAR. Sin perjuicio de las excepciones previstas en la ley, en el tratamiento se requiere la autorización previa e informada del titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.

“ARTÍCULO [32](#). CASOS EN QUE NO ES NECESARIA LA AUTORIZACIÓN. La autorización del titular no será necesaria cuando se trate de:

- a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;
- b) Datos de naturaleza pública;
- c) Casos de urgencia médica o sanitaria;
- d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;
- e) Datos relacionados con el Registro Civil de las Personas;

Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la Ley [1581](#) de 2012”.

5°. Mediante el Acuerdo [013](#) de 2019, expedido por el Consejo Directivo Nacional, se aprobó la Política General de Seguridad de la Información y Protección de Datos Personales en el SENA, la cual tiene por objeto “Determinar los lineamientos que permitan proteger la información y protección de los datos personales que adopta el Servicio Nacional de Aprendizaje (SENA), a través de acciones de aseguramiento de la información, teniendo en cuenta los requisitos legales, operativos, tecnológicos y de seguridad de la entidad, alineados con el contexto de direccionamiento estratégico y de gestión del riesgo, con el fin de asegurar el cumplimiento de la integridad, disponibilidad, legalidad y confidencialidad de la información”.

Por su parte, el Manual de la Política General de Seguridad de la Información y Protección de Datos Personales del SENA, adoptado mediante el artículo [7](#) del Acuerdo 013 de 2019, indica los lineamientos técnicos y operativos que apoyarán la gestión de la seguridad y privacidad de la información y protección de datos en la Entidad, permitiendo la integración del Sistema Integrado de Gestión y Autocontrol (SIGA) con el Subsistema de Seguridad de la Información, y llevando la implementación de los controles necesarios para salvaguardar la información del SENA desde la Dirección General hasta sus centros de formación.

Los artículos [8](#), [9](#), [10](#) y [11](#) ibídem establecen:

“ARTÍCULO [8o](#). La Dirección de Planeación y Direccionamiento Corporativo en coordinación con la Oficina de Sistemas y demás áreas funcionales dentro del ámbito de sus competencias, definirá y liderará la gestión, adopción, implementación, operación, seguimiento, mantenimiento y mejora continua de las Políticas Complementarias de Seguridad de la Información y Protección de Datos Personales”.

“ARTÍCULO [9o](#). Para el desarrollo y la implementación de la Política General de Seguridad de la Información y Protección de Datos Personales en el SENA, se emitirán las guías o documentos idóneos para la aplicación de las siguientes políticas complementarias, las cuales deben ir alineadas al Modelo Integrado de Planeación y Gestión (MIPG)...”

“ARTÍCULO [10](#). RESPONSABILIDADES. Será responsabilidad del Comité Institucional de Gestión y Desempeño del Servicio Nacional de Aprendizaje (SENA), o quien haga sus veces, asegurar la implementación y desarrollo de las Políticas de Gestión y Directrices de Seguridad y Privacidad de la Información y Protección de Datos Personales.

PARÁGRAFO. Delegar en la Dirección de Planeación y Direccionamiento Corporativo del SENA la función de presentar ante el Director General, para su aprobación y/o modificación, las políticas complementarias necesarias para la implementación y desarrollo de la Política de Seguridad de la Información y Protección de Datos Personales en el SENA”.

“ARTÍCULO [11](#). RESPONSABLE DE LA SEGURIDAD DE LA INFORMACIÓN. Será responsabilidad de la Dirección de Planeación y Direccionamiento Corporativo del SENA, en coordinación con la Oficina de Sistemas, planificar, desarrollar, gestionar y establecer los lineamientos del Manual de Seguridad y Privacidad de la Información y Protección de Datos para la Entidad.

PARÁGRAFO. Para el desarrollo de la Política Complementaria de Protección de Datos Personales se deberá tener en cuenta como mínimo las categorías o clasificaciones de datos contenidas en la Leyes 1266 de 2006, [1581](#) de 2012, [1437](#) de 2011, [1712](#) de 2014 y sus decretos reglamentarios y las normas vigentes que se expidan sobre la materia...”

CONCLUSIÓN

Teniendo en cuenta lo antes expuesto, puede concluirse:

(i) El Habeas Data es un derecho fundamental consagrado en el artículo [15](#) de la Constitución Política de 1991 cuyo objetivo es proteger la intimidad personal y familiar y el buen nombre del individuo. Dicho derecho permite actualizar y rectificar las informaciones que se haya recogido en bancos de datos de entidades públicas y/o privadas.

(ii) La Ley [1581](#) de 2012 se aplica a todas las bases de datos que almacenen y utilicen datos personales, con las excepciones a que se refiere el artículo [2](#) de la misma ley y cuando se requiere la autorización del titular de la información, tal como antes se indicó.

(iii) Cuando se registren datos personales en entidades públicas como el SENA, a los titulares que se les pide datos personales deberán ser previamente informados de manera expresa, precisa e inequívoca sobre la finalidad de la información que se requiere recolectar, los derechos que le asisten como titulares de la misma y quien tendrá a su cargo el manejo de los datos personales.

(v) Conforme con lo previsto en el artículo [2.1.1.4.1.2](#). del Decreto 1081 de 2015, cuando se trate de datos personales de carácter privado, semiprivado o sensible, sólo podrá permitirse su acceso con autorización expresa y escrita del titular de la información, salvo cuando concurra alguna de las excepciones consagradas en los artículos [6](#) y [10](#) de la Ley 1581 de 2012.

RESPUESTA PREGUNTAS

Visto lo anterior, procedemos a responder las preguntas formuladas:

¿Se puede remitir a los Despachos Regionales y Centros de Formación Profesional, la información personal de los ciudadanos que fue recopilada a través de: Google forms y la encuesta de satisfacción, incluyendo aspectos tales como: Nombre, identificación, correo electrónico y número de teléfono móvil ó fijo?.

En caso de ser positiva la respuesta anterior, ¿Cuáles serían los mecanismos para remitir, transmitir o entregar la información a las dependencias de forma segura?

¿Cuáles serían las actividades de control, compromisos, acuerdos de confidencialidad, etc. que deberían tener las dependencias que reciben la información de forma tal que se garantice la confidencialidad y el manejo de la información solamente para los fines que requiere la Entidad?

En ambos casos siempre garantizando que no se afecten los derechos de los ciudadanos.

¿Es posible entregar la información recopilada por el canal presencial y la correspondiente encuesta de medición de satisfacción a otras dependencias, para que se adelanten las investigaciones correspondientes? Al igual que en el punto anterior, ¿Cuáles serían los mecanismos para entrega y recibo de la información?

RESPUESTA: Como quedó antes expuesto, toda información personal puede ser obtenida o recolectada por cualquier medio, incluyendo los electrónicos, que pueda ser objeto de consulta posterior, siempre y cuando sea la persona, como titular del dato o de la información, quien autorice expresamente su entrega o tratamiento.

La información personal solo podrá usarse para los fines autorizados previamente por el titular de la información o dato, para lo cual deberá tenerse en cuenta que al momento en que se haya solicitado la autorización para recolección y tratamiento se le haya informado a la persona el uso que se le vaya a dar a los mismos.

Empero, la información personal del titular no podrá ser suministrada a terceros sin su previa y expresa autorización. En este caso, el texto donde se pide la autorización de datos personales - Habeas Data en la encuesta a las personas que fueron registradas en el formulario de Google, señala:

“De conformidad con lo dispuesto en la Ley [1581](#) de 2012, su Decreto Reglamentario 1377 de 2013 y el Acuerdo No [013](#) de 2019, AUTORIZO de manera libre, previa, expresa, voluntaria y debidamente informada, a que el Servicio Nacional de Aprendizaje – SENA recolecte, recaude, almacene, use, circule, suprima, procese, compile, intercambie, de tratamiento, actualice y disponga de los datos que han sido suministrados y que se han incorporado en distintas bases o bancos de datos de todo tipo en el marco de la medición de satisfacción. En este sentido, el SENA queda autorizado de manera expresa e inequívoca para mantener y manejar toda mi información personal y profesional para los fines que se encuentra legal y reglamentariamente facultado.

Sin perjuicio de lo anterior, los referidos datos no podrán ser distribuidos, comercializados, compartidos, suministrados o intercambiados con terceros, y en general, realizar actividades en las cuales se vea comprometida la confidencialidad y protección de la información recolectada, y podré en cualquier momento solicitar que la información sea modificada, actualizada o retirada de las bases de datos del SENA.

Así mismo, se me indicó que para mayor información podré consultar en cualquier momento el

Acuerdo No. [013](#) de 2019, “Por medio de la cual se aprueba la Política General de Seguridad de la Información y Protección de Datos Personales en el Servicio Nacional de Aprendizaje (SENA).” que se encuentra en la página de la Entidad: http://normograma.sena.edu.co/normograma/docs/acuerdo_sena_0013_2019.htm, la Ley [1581](#) de 2012 y el Decreto 1377 de 2013.”

Como puede apreciarse, en la encuesta de medición de satisfacción se solicitó a las personas que se registraron para que de manera libre, previa, expresa, voluntaria y debidamente informada, autorizaran al Servicio Nacional de Aprendizaje – SENA para recolectar, recaudar, almacenar, usar, circular, suprimir, procesar, compilar, intercambiar, dar tratamiento, actualizar y disponer de los datos que fueron suministrados y que se incorporaron en distintas bases o bancos de datos de todo tipo en el marco de la medición de satisfacción.

De lo anterior se deduce que el titular de la información autorizó expresa y voluntariamente para que el SENA, en tanto entidad pública y entendida como una sola unidad institucional, pueda usar, intercambiar y disponer de los datos suministrados en las distintas bases o bancos en el marco de la medición de satisfacción, datos o información personales que solo pueden usarse o manejarse para el fin para el cual fueron solicitados y autorizados.

Significa lo anterior que el SENA, bien desde la Dirección General o desde las direcciones regionales, podrá disponer, intercambiar y usar los datos que fueron suministrados y autorizados por el titular de la información para indagar o investigar sobre la participación de intermediarios en la gestión del servicio o en los trámites por los que el ciudadano acudió a la entidad, siempre y cuando estén estrechamente relacionados con la encuesta de satisfacción.

En este sentido, y frente a la actuación de posibles tramitadores, conviene señalar que los derechos de acceso, actualización, rectificación, supresión o revocación de la autorización cuando se trate de datos personales de personas naturales es gratuito y por tanto no puede exigirse o cobrarse suma alguna.

Ahora bien, la información recogida o recolectada en bases de datos debe estar protegida por medidas técnicas que garanticen su reserva y cuidado con el fin de evitar posibles adulteraciones, pérdidas, fraudes, consultas o usos indebidos y no autorizados, tal como lo establece el literal g) del artículo 4, el literal d) del artículo 17 y el literal b) del artículo 18 de la Ley 1581 de 2015.

En tal virtud, en el SENA, mediante el Acuerdo [013](#) de 2019 expedido por el Consejo Directivo Nacional, se aprobó la Política General de Seguridad de la Información y Protección de Datos Personales en el SENA.

De igual manera, en el artículo [7](#) se adoptó el Manual de Política General de Seguridad de la Información y Protección de Datos Personales en el Servicio Nacional de Aprendizaje, el cual indica los lineamientos técnicos y operativos que apoyarán la gestión de la seguridad y privacidad de la información y protección de datos en la Entidad, permitiendo la integración del Sistema Integrado de Gestión y Autocontrol (SIGA) con el Subsistema de Seguridad de la Información, y llevando la implementación de los controles necesarios para salvaguardar la información del SENA desde la Dirección General hasta sus centros de formación.

Conforme con el artículo [8](#) del Acuerdo 013 de 2019, la Dirección de Planeación y Direccionamiento Corporativo en coordinación con la Oficina de Sistemas y demás áreas funcionales dentro del ámbito de sus competencias, definirá y liderará la gestión, adopción, implementación, operación, seguimiento, mantenimiento y mejora continua de las Políticas

Complementarias de Seguridad de la Información y Protección de Datos Personales, para cuya implementación se emitirán las guías o documentos idóneos para la aplicación de políticas complementarias, las cuales deben ir alineadas al Modelo Integrado de Planeación y Gestión (MIPG).

Así pues, corresponderá a la Dirección de Planeación y Direccionamiento Corporativo del SENA, en coordinación con la Oficina de Sistemas, establecer los lineamientos técnicos y operativos que apoyarán la gestión de la seguridad y privacidad de la información y protección de datos en la Entidad, de conformidad con lo previsto en el Acuerdo [013](#) de 2019.

En caso de que al interior del SENA no existan los respectivos documentos sobre la seguridad en el tratamiento de datos personales recolectados en bases de datos de la Entidad a la luz del precitado Acuerdo [013](#) de 2019, se recomienda establecer los mecanismos y protocolos de seguridad de obligatorio cumplimiento para el personal con acceso a los datos de carácter personal y al sistema de información.

Teniendo en cuenta lo antes expuesto, sugerimos se pida el apoyo, asesoría y acompañamiento de la Dirección de Planeación y Direccionamiento Corporativo para la adopción de los mecanismos tecnológicos y los protocolos de seguridad necesarios que deban implementarse por parte de las dependencias, tanto de la Dirección General como de las direcciones regionales, para el uso, intercambio y disposición de la información suministrada en la encuesta de medición de satisfacción en procura de la protección de las bases de datos donde repose la información recolectada, con el fin exclusivo de indagar sobre las actuaciones de tramitadores en el marco de dicha encuesta, acorde con la autorización impartida por el titular de los datos personales.

El presente concepto se rinde de conformidad con el alcance dispuesto en el artículo [28](#) del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, incorporado por la Ley [1755](#) de 2015. Lo anterior no sin advertir, que el mismo se encuentra sujeto a las modificaciones legales y jurisprudenciales que se expidan y acojan dentro del asunto.

Cordial saludo,

ANTONIO JOSÉ TRUJILLO ILLERA

Coordinador Grupo de Conceptos Jurídicos y

Producción Normativa - Dirección Jurídica

Dirección General



Disposiciones analizadas por Avance Jurídico Casa Editorial Ltda.

Normograma del Sena

ISSN Pendiente

Última actualización: 20 de abril de 2024 - (Diario Oficial No. 52.716 - 3 de abril de 2024)



logo