CONCEPTO 60126 DE 2018

(octubre 12)

<Fuente: Archivo interno entidad emisora>

SERVICIO NACIONAL DE APRENDIZAJE - SENA

ASUNTO: Los mailing (marketing directos) enviados por el correo institucional de la entidad/habeas data.

En atención a su comunicación, remitida mediante correo electrónico de fecha 04 de octubre de 2018, en la cual solicita informar sobre concepto jurídico; me permito manifestarle:

ALCANCE DE LOS CONCEPTOS JURÍDICOS

Es pertinente señalar que 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.

Finalmente, es pertinente recordar lo dispuesto en la Circular No. 00028 de 2013, para que a futuro sea tenida en cuenta por el personal de esa dependencia, y cuyo acápite pertinente señala: "[…] me permito informar que a partir de la fecha la asesoría y solicitudes de conceptos a la Dirección Jurídica, deberán ser radicados en el aplicativo Onbase y canalizados a través de la Secretaría General, Directores de Área, Jefes de Oficina, Directores Regionales, Subdirectores de Centro y Coordinadores de Grupo".

ANTECEDENTES

Señala quien consulta:

[…] Con base en la reunión sostenida el mes anterior, en el cual hablamos sobre los correos electrónicos (mailings), enviados por la Entidad a funcionarios, contratistas y aprendices a cuentas de dominio @sena.edu.co y @misena.edu.co, les agradezco indicarme por esta vía si el SENA debe pedir permiso de los destinatarios o si, por el contrario, puede seguirlo efectuando como lo ha venido haciendo.

CONCEPTO JURÍDICO

i. HABEAS DATA

La Constitución Política de 1991, dispuso en cuanto al manejo de la información lo siguiente:

ARTICULO 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. (Subraya fuera de texto)

En consecuencia, el Estado debe respetar la intimidad de las personas y hacer respetar dicha información, igualmente las personas tienen derecho a conocer el tratamiento que le dan en las bases de datos públicas y privadas, de las cuales hacen parte.

La Corte Constitucional se pronunció en la sentencia T-729 de 2002, definiendo así el habeas data:

[…] El derecho fundamental al habeas data, es aquel que otorga la facultad al titular de datos personales, de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición, actualización, y certificación de los datos, así como la limitación en la posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios que informan el proceso de administración de bases de datos personales.

La Ley 1266 de 2008, "por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones", inicialmente se refirió ala las bases de datos y manejo de información de naturaleza financiera, comercial y de servicios.

En concordancia con lo anterior, la Ley Estatutaria 1581 de 2012, "por la cual se dictan disposiciones generales para la protección de datos personales", dispuso:

ARTÍCULO 1. Objeto. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

En el mismo sentido, el artículo 3 de la norma encita, trae las siguientes definiciones pertinentes y necesarias en el caso que nos ocupa:

ARTÍCULO 3. Definiciones. Para los efectos de la presente ley, se entiende por:

a) Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales;

b) Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento;

c) Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables;

d) 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;

e) 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

f) Titular: Persona natural cuyos datos personales sean objeto de Tratamiento;

g) Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Subraya fuera de texto)

En concordancia con lo anterior, y dentro del ámbito de aplicación, se establece una protección especial a la entrega de bases de datos, así:

ARTÍCULO 2. Ámbito de aplicación. Los principios y disposiciones contenidas en la presente ley 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 régimen de protección de datos personales que se establece en la presente ley no será de aplicación:

a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.

Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley;

b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo;

c) A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia;

d) A las bases de datos y archivos de información periodística y otros contenidos editoriales;

e) A las bases de datos y archivos regulados por la Ley 1266 de 2008;

f) A las bases de datos y archivos regulados por la Ley 79 de 1993.

Parágrafo. Los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal. En el evento que la normatividad especial que regule las bases de datos exceptuadas prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley. (Subraya fuera de texto)

A su turno, el Decreto 1377 de 2013, “por el cual se reglamenta parcialmente la Ley 1581 de

2012”, en el artículo 4, estableció sobre la recolección de datos personales, en desarrollo de los principios de finalidad y libertad, que la recolección de datos deberá limitarse a aquellos datos personales que son pertinentes y adecuados para la finalidad para la cual son recolectados o requeridos conforme a la normatividad vigente. Reza la norma en comento:

ARTÍCULO 4. Recolección de los datos personales. En desarrollo de los principios de finalidad y libertad, la recolección de datos deberá limitarse a aquellos datos personales que son pertinentes y adecuados para la finalidad para la cual son recolectados o requeridos conforme a la normatividad vigente. Salvo en los casos expresamente previstos en la ley, no se podrán recolectar datos personales sin autorización del Titular

A solicitud de la Superintendencia de Industria y Comercio, los Responsables deberán proveer una descripción de los procedimientos usados para la recolección, almacenamiento, uso, circulación y supresión de información, como también la descripción de las finalidades para las cuales la información es recolectada y una explicación sobre la necesidad de recolectar los datos en cada caso.

No se podrán utilizar medios engañosos o fraudulentos para recolectar y realizar Tratamiento de datos personales.

ARTÍCULO 5. Autorización. El Responsable del Tratamiento deberá adoptar procedimientos para solicitar, a más tardar en el momento de la recolección de sus datos, la autorización del Titular para el Tratamiento de los mismos e informarle los datos personales que serán recolectados así como todas las finalidades específicas del Tratamiento para las cuales se obtiene el consentimiento.

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

En caso de haber cambios sustanciales en el contenido de las políticas del Tratamiento a que se refiere el Capítulo III de este decreto, referidos a la identificación del Responsable y a la finalidad del Tratamiento de los datos personales, los cuales puedan afectar el contenido de la autorización, el Responsable del Tratamiento debe comunicar estos cambios al Titular antes de o a más tardar al momento de implementar las nuevas políticas. Además, deberá obtener del Titular una nueva autorización cuando el cambio se refiera a la finalidad del Tratamiento. (Subraya fuera de texto)

En conclusión y reiterando lo ya manifestado por el Grupo de Conceptos y Producción Normativa, “[…] los datos personales de los titulares no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento”. Al respecto es preciso señalar la existencia de datos que afectan la intimidad del titular o cuyo uso indebido genera discriminación, es decir el caso de los datos sensibles, cuyo tratamiento se encuentra prohibido. (Artículo 6 de la Ley 1581 de 2012)

La Corte Constitucional, en concordancia con lo manifestado por la Carta Fundamental y la normatividad expuesta, señaló en sentencia de control abstracto de constitucionalidad C-748 de 2011, señaló lo siguiente:

[…] DERECHO AL HABEAS DATA-Concepto/DERECHO AL HABEAS DATA-Líneas

interpretativas en la jurisprudencia constitucional/DERECHO AL HABEAS DATA-Fundamental autónomo. En la jurisprudencia constitucional, el derecho al habeas data fue primero interpretado como una garantía del derecho a la intimidad, de allí que se hablara de la protección de los datos que pertenecen a la vida privada y familiar, entendida como la esfera individual impenetrable en la que cada cual puede realizar su proyecto de vida y en la que ni el Estado ni otros particulares pueden interferir. También, desde los primeros años de la nueva Carta, surgió al interior de la Corte una segunda línea interpretativa que consideraba el habeas data una manifestación del libre desarrollo de la personalidad. Según esta línea, el habeas data tiene su fundamento último "(…) en el ámbito de autodeterminación y libertad que el ordenamiento jurídico reconoce al sujeto como condición indispensable para el libre desarrollo de la personalidad y en homenaje justiciero a su dignidad. Ya a partir de 1995, surge una tercera línea interpretativa que es la que ha prevalecido desde entonces y que apunta al habeas data como un derecho autónomo, en que el núcleo del derecho al habeas data está compuesto por la autodeterminación informática y la libertad –incluida la libertad económica. Este derecho como fundamental autónomo, requiere para su efectiva protección de mecanismos que lo garanticen, los cuales no sólo deben pender de los jueces, sino de una institucionalidad administrativa que además del control y vigilancia tanto para los sujetos de derecho público como privado, aseguren la observancia efectiva de la protección de datos y, en razón de su carácter técnico, tenga la capacidad de fijar política pública en la materia, sin injerencias políticas para el cumplimiento de esas decisiones.

[…] DERECHO AL HABEAS DATA-Contenidos mínimos. Dentro de las prerrogativas o contenidos mínimos que se desprenden del derecho al habeas data encontramos por lo menos las siguientes: (i) el derecho de las personas a conocer –acceso- la información que sobre ellas están recogidas en bases de datos, lo que conlleva el acceso a las bases de datos donde se encuentra dicha información; (ii) el derecho a incluir nuevos datos con el fin de que se provea una imagen completa del titular; (iii) el derecho a actualizar la información, es decir, a poner al día el contenido de dichas bases de datos; (iv) el derecho a que la información contenida en bases de datos sea rectificada o corregida, de tal manera que concuerde con la realidad; (v) el derecho a excluir información de una base de datos, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular –salvo las excepciones previstas en la normativa. (Subraya fuera de texto)

De otra parte, también la Corte Constitucional, en sentencia T-729 de 2002, señaló:

[…] El derecho fundamental al habeas data, es aquel que otorga la facultad al titular de datos personales, de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición, actualización, y certificación de los datos, así como la limitación en la posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios que informan el proceso de administración de bases de datos personales.

[…] el principio de libertad, los datos personales sólo pueden ser registrados y divulgados con el consentimiento libre, previo y expreso del titular, de tal forma que se encuentra prohibida la obtención y divulgación de los mismos de manera ilícita (ya sea sin la previa autorización del titular o en ausencia de mandato legal o judicial). En este sentido por ejemplo, se encuentra prohibida su enajenación o cesión por cualquier tipo contractual.

Según el principio de necesidad, los datos personales registrados deben ser los estrictamente necesarios para el cumplimiento de las finalidades perseguidas con la base de datos de que se trate, de tal forma que se encuentra prohibido el registro y divulgación de datos que no guarden

estrecha relación con el objetivo de la base de datos.

Según el principio de veracidad los datos personales deben obedecer a situaciones reales, deben ser ciertos, de tal forma que se encuentra prohibida la administración de datos falsos o erróneos.

Según el principio de integridad, estrechamente ligado al de veracidad, la información que se registre o se divulgue a partir del suministro de datos personales debe ser completa, de tal forma que se encuentra prohibido el registro y divulgación de datos parciales, incompletos o fraccionados. Con todo, salvo casos excepcionales, la integridad no significa que una única base de datos pueda compilar datos que, sin valerse de otras bases de datos, permitan realizar un perfil completo de las personas.

Según el principio de finalidad, tanto el acopio, el procesamiento y la divulgación de los datos personales, debe obedecer a una finalidad constitucionalmente legítima, definida de manera clara, suficiente y previa; de tal forma que queda prohibida la recopilación de datos sin la clara especificación acerca de la finalidad de los mismos, así como el uso o divulgación de datos para una finalidad diferente a la inicialmente prevista.

Según el principio de utilidad, tanto el acopio, el procesamiento y la divulgación de los datos personales, debe cumplir una función determinada, como expresión del ejercicio legítimo del derecho a la administración de los mismos; por ello, está prohibida la divulgación de datos que, al carecer de función, no obedezca a una utilidad clara o determinable.

Según el principio de circulación restringida, estrechamente ligado al de finalidad, la divulgación y circulación de la información está sometida a los límites específicos determinados por el objeto de la base de datos, por la autorización del titular y por el principio de finalidad, de tal forma que queda prohibida la divulgación indiscriminada de los datos personales.

Según el principio de incorporación, cuando de la inclusión de datos personales en determinadas bases, deriven situaciones ventajosas para el titular, la entidad administradora de datos estará en la obligación de incorporarlos, si el titular reúne los requisitos que el orden jurídico exija para tales efectos, de tal forma que queda prohibido negar la incorporación injustificada a la base de datos.

Según el principio de caducidad, la información desfavorable al titular debe ser retirada de las bases de datos siguiendo criterios de razonabilidad y oportunidad, de tal forma que queda prohibida la conservación indefinida de los datos después que han desaparecido las causas que justificaron su acopio y administración.

Según el principio de individualidad, las administradoras deben mantener separadamente las bases de datos que se encuentren bajo su administración, de tal forma que queda prohibida la conducta dirigida a facilitar cruce de datos a partir de la acumulación de informaciones provenientes de diferentes bases de datos.

Además de las obligaciones derivadas de los principios rectores del proceso de administración de bases de datos personales, existen otros que tienen su origen directo en normas constitucionales y legales, sobre todo lo relativo (sic) a la obligación de diligencia en el manejo de los datos personales y la obligación de indemnizar los perjuicios causados por las posibles fallas en el proceso de administración. (Subraya fuera de texto)

Es así como, la Corte Constitucional frente al tema del administrador de bases de datos reiteró

por medio de la Sentencia T-176A/14:

[…] LOS PRINCIPIOS Y LAS REGLAS QUE DEBE SEGUIR EL ADMINISTRADOR DE BASES DE DATOS. REITERACIÓN JURISPRUDENCIAL.

2.5.1. Esta Corte en materia de habeas data ha sido constante en precisar que la administración de toda base de datos personales está sometida a los llamados principios de administración de datos personales. (…)

2.5.3. Las Sentencias C-748 de 2011 y C-1011 de 2008 son la concreción de la jurisprudencia que, desde las Sentencias T-729 de 2002 y C-185 de 2003, se había perfilado por esta Corte sobre la obligatoriedad de los principios a que toda actividad de administración de datos personales debe someterse.

2.5.4. Entre los mencionados principios de la administración de datos personales encontramos: i) los principios de finalidad; ii) necesidad; iii) utilidad; y iv) circulación restringida, los cuales prescriben una serie ineludible de deberes en relación con las actividades de recolección, procesamiento y divulgación de la información personal.

2.5.5. Según el principio de finalidad, tales actividades "deben obedecer a un fin constitucionalmente legítimo (…) definido de forma clara, suficiente y previa". Por lo cual, está prohibida, por un lado "la recopilación de información personal sin que se establezca el objetivo de su incorporación a la base de datos (…)"y por el otro "la recolección, procesamiento y divulgación de información personal para un propósito diferente al inicialmente previsto (…)"

2.5.6. Según el principio de necesidad, la administración de "la información personal concernida debe ser aquella estrictamente necesaria para el cumplimiento de los fines de la base de datos"

2.5.7. Según el principio de utilidad, la administración de información personal debe "cumplir una función determinada, acorde con el ejercicio legítimo de la administración de los datos personales. Por lo cual queda proscrita la divulgación de datos que, al carecer de función, no obedezca a una utilidad clara y suficientemente determinable"

2.5.8. El principio de circulación restringida ordena que toda actividad de administración de información personal esté sometida "a los límites específicos determinados por el objeto de la base de datos (…) y por el principio de finalidad. Por lo cual, está prohibida la divulgación indiscriminada de datos personales"

2.5.9. Para la Corte, los anteriores principios tienen el propósito de circunscribir la actividad de administración de información personal contenida en bases de datos, pues al limitar el ejercicio de las competencias de los administradores de bases de datos, definen el margen de su actuación y son una garantía para las libertades de los sujetos concernidos por la información administrada. En términos normativos, son la concreción legal y jurisprudencial del mandato del inciso 2o, del artículo 15 de la Constitución que estable que "en la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución".

En este contexto, se ha concluido lo siguiente:

[…]

1. La información que se pretenda entregar a cualquier Entidad, que se encuentre contenida en alguna base de datos deberá contar con autorización expresa del titular.

2. Las bases de datos que contengan información de adolescentes se deberá compartir conforme a lo señalado en el acápite normativo.

3. La información que podría suministrar la Entidad en caso de no contar con la autorización del titular será estadística o tipo informe.

En caso que se requiera la información para el cumplimiento de sus funciones administrativas alguna entidad pública, deberá ser conforme con lo señalado en el Decreto 235 de 2010, "por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas", que señala:

ARTÍCULO 2. Para efectos del intercambio de Información, las entidades a que hace referencia el artículo anterior deberán establecer mecanismos magnéticos, electrónicos o telemáticos para integrar, compartir y/o suministrar la información que por mandato legal se requiere, o permitir el acceso total dentro del marco de la Constitución y el derecho fundamental a la intimidad, a las bases de datos completas que requieran otras entidades para el ejercicio de sus funciones.

Y, en concordancia con lo indicado en el Decreto 2280 de 2010, "por el cual se modifica el artículo 3o del Decreto 235 de 2010", que dispuso:

ARTÍCULO 1. Modificase el artículo 3 del Decreto 235 de 2010, el cual quedará así:

ARTÍCULO 3. Para efectos de formalizar el intercambio de información, de manera ágil, oportuna y confiable, las entidades públicas o los particulares encargados de una función administrativa podrán emplear el mecanismo que consideren idóneo para el efecto, tales como cronograma de entrega, plan de trabajo, protocolo o convenio, entre otros." (Subrayado fuera de texto).

Finalmente, es preciso indicar que si la base de datos de la cual se pretende su uso, incluye datos de menores- adolescentes, se tiene un tratamiento preferencial según lo reglado en el artículo 7 de la precitada Ley Estatutaria1581 de 2012:

ARTÍCULO 7. Derechos de los niños, niñas y adolescentes. En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.

Queda proscrito el Tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública

Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del Tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás. El Gobierno Nacional reglamentará la materia, dentro de los seis (6) meses siguientes a la promulgación de esta ley.

Así que conforme a la norma mencionada al parecer cualquier tratamiento de datos personales de menores-adolescentes está prohibido. Sin embargo, a través de la sentencia de control abstracto de constitucionalidad C-748 de 2011, se estableció:

[…] Es importante referir brevemente qué se entiende por niño, niña y adolescente en el

ordenamiento jurídico colombiano. En desarrollo de este concepto, el Código de la Infancia y la Adolescencia, en su artículo 3o, estableció: "(…) se entiende por niño o niña las personas entre los 0 y 12 años, y por adolescente las personas entre 12 y 18 años de edad". La anterior definición fue declarada exequible por esta Corporación. Además es consonante con la definición en sentido amplio que contiene la Convención sobre los derechos del niño como "(…) todo ser humano menor de dieciocho años de edad (…)".

[…] En definitiva, (i) el principio del interés superior de los niños, las niñas y adolescentes se realiza en el estudio de cada caso en particular y tiene por fin asegurar su desarrollo integral; (ii) este principio, además, persigue la realización efectiva de los derechos fundamentales de los menores de 18 años y también resguardarlos de los riesgos prohibidos que amenacen su desarrollo armónico. Estos riesgos no se agotan en los que enuncia la ley sino que también deben analizarse en el estudio de cada caso particular; (iii) debe propenderse por encontrar un equilibrio entre los derechos de los padres o sus representantes legales y los de los niños, las niñas y adolescentes. Sin embargo, cuando dicha armonización no sea posible, deberán prevalecer las garantías superiores de los menores de 18 años. En otras palabras, siempre que prevalezcan los derechos de los padres, es porque se ha entendido que ésta es la mejor manera de darle aplicación al principio del interés superior de los niños, las niñas y adolescentes.

La calidad de sujetos de especial protección constitucional de los menores de dieciocho años tiene su fundamento en la situación de vulnerabilidad e indefensión en la que se encuentran, pues su desarrollo físico, mental y emocional está en proceso de alcanzar la madurez requerida para la toma de decisiones y participación autónoma dentro de la sociedad. El grado de vulnerabilidad e indefensión tiene diferentes grados y se da partir de todos los procesos de interacción que los menores de 18 años deben realizar con su entorno físico y social para el desarrollo de su personalidad. Por lo anterior, el Estado, la sociedad y la familia deben brindar una protección especial en todos los ámbitos de la vida de los niños, niñas y adolescentes, en aras de garantizar su desarrollo armónico e integral.

Adicional a lo expuesto, la protección constitucional reforzada de la cual son titulares los niños, las niñas y adolescentes tiene su sustento en (i) el respeto de su dignidad humana, y (ii) la importancia de construir un futuro promisorio para la comunidad mediante la efectividad de todos sus derechos fundamentales.

En este orden de ideas, esta Sala encuentra que en el caso concreto del tratamiento de los datos de los niños, niñas y adolescentes, existe un riesgo prohibido que esta población en situación de vulnerabilidad está expuesta a sufrir, principalmente por la desbordante evolución de los medios informáticos, entre los que se encuentran la Internet y las redes sociales. Si bien, el acceso a los distintos sistemas de comunicación, les permite disfrutar de todos sus beneficios y ventajas, también su mal uso puede generar un conflicto en el ejercicio y efectividad de sus derechos fundamentales al buen nombre, al honor, a la intimidad, entre otros. El anterior planteamiento fue abordado en el Memorando sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes, adoptado en Montevideo el 28 de julio de 2009. Si bien, este documento no integra el denominado bloque de constitucionalidad y por tanto sus recomendaciones no son vinculantes para el Estado colombiano, constituye un documento valioso en torno al tema de la protección de datos personales de los niños, las niñas y adolescentes. (Subraya fuera de texto)

Igualmente, en el tema específico relacionado con estas bases de datos que incluyen información de menores-adolescentes, de acuerdo con el artículo 7 ibídem, manifestó:

[…] En cuanto al inciso 3o del artículo 7o del proyecto debe también resaltarse que no sólo el Estado y las entidades educativas deben desarrollar acciones para evitar el uso inadecuado de los datos personales de los menores de 18 años sino que también son responsables en el aseguramiento de dicha garantía (i) los progenitores u otras personas que se encuentren a cargo de su cuidado y los educadores; (ii) el legislador, quien debe asegurarse que en cumplimiento de sus funciones legislativas, específicamente, en lo referente al tratamiento de los datos personales de los menores de 18 años, dicha normativa no deje de contener las medidas adecuadas de protección para garantizar su desarrollo armónico e integral, y la efectividad de sus derechos fundamentales contenidos en la Constitución Política y en los estándares internacionales que existen sobre la materia; (iii) el sistema judicial; específicamente los servidores públicos deben proteger los derechos derivados del uso de los datos personales de los menores de 18 años observando los estándares internacionales o documentos especializados sobre la materia; (iv) los medios de comunicación; (v) las empresas que proveen los servicios de acceso a la Internet, desarrollan las aplicaciones o las redes sociales digitales, a quienes se advierte que deben comprometerse en la defensa de los derechos fundamentales de los niños, niñas y adolescentes

ii. INFORMACIÓN PÚBLICA Y RESERVADA

En forma general, es pertinente señalar que la información reservada y confidencial es una excepción al principio de publicidad. La Corte Constitucional en sentencia C-274 de 2013, señaló:

[…] DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA-Contenido y alcance. Es titular del derecho a acceder a la información pública toda persona, sin exigir ninguna cualificación o interés particular para que se entienda que tiene derecho a solicitar y a recibir dicha información de conformidad con las reglas que establece la Constitución y el proyecto de ley. Esta disposición se ajusta a los parámetros constitucionales del derecho de petición, de información y del libre acceso a los documentos públicos, a los principios de la función pública, que consagran los artículos 20, 23, 74 y 209 de la Carta.

[…] PUBLICIDAD DE LA INFORMACIÓN-Reglas jurisprudenciales que deben cumplirse al establecer restricciones. Es relevante recordar las reglas jurisprudencias que deben cumplirse al establecer restricciones a la publicidad de la información, a fin de dar claridad a las condiciones que deben atenderse cuando se pretenda oponerse a la publicidad de un documento o información, dado que tales requisitos fueron recogidos de manera sumaria en esta disposición. En la sentencia T-451 de 2011 la Corte resumió los requisitos en los siguientes términos: Las normas que limitan el derecho de acceso a la información deben ser interpretadas de manera restrictiva y toda limitación debe estar adecuadamente motivada. A este respecto la Corte ha señalado que existe una clara obligación del servidor público de motivar la decisión que niega el acceso a información pública y tal motivación debe reunir los requisitos establecidos por la Constitución y la ley. En particular debe indicar expresamente la norma en la cual se funda la reserva, por esta vía el asunto puede ser sometido a controles disciplinarios, administrativos e incluso judiciales. Los límites del derecho de acceso a la información pública debe estar fijados en la ley, por lo tanto no son admisibles las reservas que tienen origen en normas que no tengan esta naturaleza, por ejemplo actos administrativos. No son admisibles las normas genéricas o vagas en materia de restricción del derecho de acceso a la información porque pueden convertirse en una especie de habilitación general a las autoridades para mantener en secreto toda la información que discrecionalmente consideren adecuado. La ley debe establecer con claridad y precisión (i) el tipo de información que puede ser objeto de reserva, (ii) las condiciones en las

cuales dicha reserva puede oponerse a los ciudadanos, (iii) las autoridades que pueden aplicarla y (iv) los sistemas de control que operan sobre las actuaciones que por tal razón permanecen reservadas. Los límites al derecho de acceso a la información sólo serán constitucionalmente legítimos si tienen la finalidad de proteger derechos fundamentales o bienes constitucionalmente valiosos como (i) la seguridad nacional, (ii) el orden público, (iii) la salud pública y (iv) los derechos fundamentales y si además resultan idóneos (adecuados para proteger la finalidad constitucionalmente legítima) y necesarios para tal finalidad (principio de proporcionalidad en sentido estricto), es decir, las medidas que establecen una excepción a la publicidad de la información pública deben ser objeto de un juicio de proporcionalidad. Así, por ejemplo, se han considerado legítimas las reservas establecidas (1) para garantizar la defensa de los derechos fundamentales de terceras personas que puedan resultar desproporcionadamente afectados por la publicidad de una información; (2) para garantizar la seguridad y defensa nacional; (3) para asegurar la eficacia de las investigaciones estatales de carácter penal, disciplinario, aduanero o cambiario; (4) con el fin de garantizar secretos comerciales e industriales. (Subraya fuera de texto)

De acuerdo con la Ley 1755 de 2015, "por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo", y la Ley 1437 de 2011- Código de Procedimiento Administrativo y de lo Contencioso Administrativo-CPACA, se tiene como información reservada:

ARTÍCULO 24. Informaciones y documentos reservados. Solo tendrán carácter reservado las informaciones y documentos expresamente sometidos a reserva por la Constitución Política o la ley, y en especial:

1. Los relacionados con la defensa o seguridad nacionales.

2. Las instrucciones en materia diplomática o sobre negociaciones reservadas.

3. Los que involucren derechos a la privacidad e intimidad de las personas, incluidas en las hojas de vida, la historia laboral y los expedientes pensionales y demás registros de personal que obren en los archivos de las instituciones públicas o privadas, así como la historia clínica.

4. Los relativos a las condiciones financieras de las operaciones de crédito público y tesorería que realice la nación, así como a los estudios técnicos de valoración de los activos de la nación. Estos documentos e informaciones estarán sometidos a reserva por un término de seis (6) meses contados a partir de la realización de la respectiva operación.

5. Los datos referentes a la información financiera y comercial, en los términos de la Ley Estatutaria 1266 de 2008.

6. Los protegidos por el secreto comercial o industrial, así como los planes estratégicos de las empresas públicas de servicios públicos.

7. Los amparados por el secreto profesional.

8. Los datos genéticos humanos.

Parágrafo. Para efecto de la solicitud de información de carácter reservado, enunciada en los numerales 3, 5, 6 y 7 solo podrá ser solicitada por el titular de la información, por sus apoderados o por personas autorizadas con facultad expresa para acceder a esa información.

En este orden de ideas, se tiene que no toda la información es pública, además, puede darse el rechazo de las peticiones de información por motivo de reserva. Así tales decisiones deben ser motivadas e indicar las disposiciones legales que impiden la entrega de la información o documentos pertinentes. Esta decisión de rechazo debe notificarse al peticionario y contra ella no procede recurso alguno, salvo el de insistencia, que se encuentra consagrado en el artículo 26 de la norma ibídem. Reza la norma:

ARTÍCULO 26. Insistencia del solicitante en caso de reserva. Si la persona interesada insistiere en su petición de información o de documentos ante la autoridad que invoca la reserva, corresponderá al Tribunal Administrativo con jurisdicción en el lugar donde se encuentren los documentos, si se trata de autoridades nacionales, departamentales o del Distrito Capital de Bogotá, o al juez administrativo si se trata de autoridades distritales y municipales decidir en única instancia si se niega o se acepta, total o parcialmente la petición formulada.

Para ello, el funcionario respectivo enviará la documentación correspondiente al tribunal o al juez administrativo, el cual decidirá dentro de los diez (10) días siguientes. Este término se interrumpirá en los siguientes casos:

1. Cuando el tribunal o el juez administrativo solicite copia o fotocopia de los documentos sobre cuya divulgación deba decidir, o cualquier otra información que requieran, y hasta la fecha en la cual las reciba oficialmente.

2. Cuando la autoridad solicite, a la sección del Consejo de Estado que el reglamento disponga, asumir conocimiento del asunto en atención a su importancia jurídica o con el objeto de unificar criterios sobre el tema. Si al cabo de cinco (5) días la sección guarda silencio, o decide no avocar conocimiento, la actuación continuará ante el respectivo tribunal o juzgado administrativo.

Parágrafo. El recurso de insistencia deberá interponerse por escrito y sustentado en la diligencia de notificación, o dentro de los diez (10) días siguientes a ella.

La 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”, tiene por objeto, regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información. En este sentido, dispone respecto a la información reservada o no pública:

ARTÍCULO 18. Información exceptuada por daño de derechos a personas naturales o jurídicas. Corregido por el art. 2, Decreto Nacional 1494 de 2015 Es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito, siempre que el acceso pudiere causar un daño a los siguientes derechos:

a) Corregido por el art. 1, Decreto Nacional 2199 de 2015 El derecho de toda persona a la intimidad, bajo las limitaciones propias que impone la condición de servidor público, en concordancia con lo estipulado;

b) El derecho de toda persona a la vida, la salud o la seguridad;

c) Los secretos comerciales, industriales y profesionales, así como los estipulados en el parágrafo del artículo 77 de la Ley 1474 de 2011.

Parágrafo. Estas excepciones tienen una duración ilimitada y no deberán aplicarse cuando la

persona natural o jurídica ha consentido en la revelación de sus datos personales o privados o bien cuando es claro que la información fue entregada como parte de aquella información que debe estar bajo el régimen de publicidad aplicable.

ARTÍCULO 19. Información exceptuada por daño a los intereses públicos. Es toda aquella información pública reservada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito en las siguientes circunstancias, siempre que dicho acceso estuviere expresamente prohibido por una norma legal o constitucional:

a) La defensa y seguridad nacional;

b) La seguridad pública;

c) Las relaciones internacionales;

d) La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso;

e) El debido proceso y la igualdad de las partes en los procesos judiciales;

f) La administración efectiva de la justicia;

g) Los derechos de la infancia y la adolescencia;

h) La estabilidad macroeconómica y financiera del país;

i) La salud pública.

Parágrafo. Se exceptúan también los documentos que contengan las opiniones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos.

Conforme con la normatividad expuesta, tenemos que cierto tipo de información está afectada de reserva legal, y en tal virtud, puede negarse el acceso a la misma, siendo un deber de quien tiene su custodia proteger la información. El artículo 4 de la Ley 1712 consagra que toda la información que esté en posesión, custodia o bajo control de los sujetos obligados es pública. Pero existen excepciones con el fin de evitar que se causen daños a derechos de las personas o a bienes públicos.

Los criterios para asignar la calificación a las categorías de información son aquellos indicados por la Ley 1712 de 2014 que fue reglamentada con el Decreto 103 de 2015 y que además son reiterados en el Decreto reglamentario Único del Sector Presidencia de la República. De igual forma se aconseja apoyar éstos conceptos de calificación de la información de acuerdo a indicaciones proporcionadas por la Ley 594 de 2000 y decretos reglamentarios (Ley General de Archivos) y la Ley Estatutaria 1581 de 2012 y decretos reglamentarios (sobre el tratamiento de los datos personales). [4]

iii. CONCEPTOS ANTERIORES RENDIDOS POR EL GRUPO

Se encuentra que este Grupo emitió, posterior al año 2015, concepto dentro del NIS: 2017-02-377159, en atención a la comunicación radicado No. 8-2017-061231 del 21 de noviembre de 2017, el cual se encuentra publicado en el normograma y que concluyó:

[…] CONCLUSIÓN

4. La información que se pretenda entregar a cualquier Entidad, que se encuentre contenida en alguna base de datos deberá contar con autorización expresa del titular por tratar con información de adolescentes.

5. Las bases de datos que contengan información de adolescentes se deberá compartir conforme a lo señalado en el acápite normativo.

6. La información que podría suministrar la Entidad en caso de no contar con la autorización del titular será estadística o tipo informe.

7. En caso que se requiera la información para el cumplimiento de sus funciones administrativas alguna entidad pública, deberá regirse conforme a lo señalado en el Decreto 235 de 2010 que señala:

“Artículo 2o Para efectos del intercambio de Información, las entidades a que hace referencia el artículo anterior deberán establecer mecanismos magnéticos, electrónicos o telemáticos para integrar, compartir y/o suministrar la información que por mandato legal se requiere, o permitir el acceso total dentro del marco de la Constitución y el derecho fundamental a la intimidad, a las bases de datos completas que requieran otras entidades para el ejercicio de sus funciones.

Y, en concordancia con lo indicado en el Decreto 2280 de 2010:

“ARTÍCULO PRIMERO. Modificase el artículo 3 del Decreto 235 de 2010, el cual quedará así:

Artículo 3o. Para efectos de formalizar el intercambio de información, de manera ágil, oportuna y confiable, las entidades públicas o los particulares encargados de una función administrativa podrán emplear el mecanismo que consideren idóneo para el efecto, tales como cronograma de entrega, plan de trabajo, protocolo o convenio, entre otros." (Subrayado fuera de texto).

Igualmente, se encuentra, el concepto emitido bajo el NIS No. 2017-02-377159, dentro del radicado No. 8-2017-061231 del 21 de noviembre de 2017, el cual también analizó el tema ante solicitud de la Dirección de Empleo y trabajo, e igualmente se concluyó:

[…] CONCLUSIÓN

1. La información que se pretenda entregar a cualquier Entidad, que se encuentre contenida en alguna base de datos deberá contar con autorización expresa del titular por tratar con información de adolescentes.

2. Las bases de datos que contengan información de adolescentes se deberá compartir conforme a lo señalado en el acápite normativo.

3. La información que podría suministrar la Entidad en caso de no contar con la autorización del titular será estadística o tipo informe.

4. En caso que se requiera la información para el cumplimiento de sus funciones administrativas alguna entidad pública, deberá regirse conforme a lo señalado en el Decreto 235 de 2010 que señala:

“Artículo 2o Para efectos del intercambio de Información, las entidades a que hace referencia el artículo anterior deberán establecer mecanismos magnéticos, electrónicos o telemáticos para integrar, compartir y/o suministrar la información que por mandato legal se requiere, o permitir

el acceso total dentro del marco de la Constitución y el derecho fundamental a la intimidad, a las bases de datos completas que requieran otras entidades para el ejercicio de sus funciones.

Y, en concordancia con lo indicado en el Decreto 2280 de 2010:

“ARTÍCULO PRIMERO. Modificase el artículo 3 del Decreto 235 de 2010, el cual quedará así:

Artículo 3o. Para efectos de formalizar el intercambio de información, de manera ágil, oportuna y confiable, las entidades públicas o los particulares encargados de una función administrativa podrán emplear el mecanismo que consideren idóneo para el efecto, tales como cronograma de entrega, plan de trabajo, protocolo o convenio, entre otros." (Subrayado fuera de texto).

iv. MAILING

Un mailing es un correo directo, una campaña de mailing consiste en enviar publicidad de manera masiva por correo convencional o electrónico, principalmente un folleto publicitario con una carta personalizada, aunque el mailing actualmente se propaga más en la actualidad por correo electrónico.

No hay que confundir el mailing con dos conceptos:

- El spam. El mailing es correo publicitario masivo, pero no es correo no deseado, ya que las personas se habrán registrado a un boletín de novedades o a un servicio de envío de emails publicitarios masivos por el que reciben este email. Una campaña de spam (correo no deseado) no se le puede confundir con una campaña de mailing.

- El buzoneo. El mailing no es buzoneo, si se envía la publicidad por correo convencional de manera masiva y no se reparte casa por casa a mano como sucede en el buzoneo.

La ventaja del mailing es que ofrece un medio de publicidad para las empresas muy económico, sobre todo por correo electrónico ya que ahorra los gastos de papel y gastos de envío, y en muchas ocasiones efectivo ya que se consiguen ventas y promoción de bienes y servicios con este sistema. Una de las desventajas es que muchas personas no abrirán la publicidad o no les parecerá interesante, de manera que muchos correos quedarán sin abrir y sin resultados.

La campaña de mailing se basa en una base de datos, por lo que es importante que esta base de datos esté constantemente actualizada para ofrecer unos mejores resultados, pues de nada sirve tener datos que ya no son válidos o incorrectos. Para que la campaña de mailing sea un tipo de marketing directoefectivo se deben tener en cuenta una serie de parámetros, aunque lo más importante es saber dar con el potencial cliente/destinatario de manera directa e incitando a ser leído o conocer la información, con un mensaje directo y personal, una motivación para leer la publicidad y ofrecer un interés en el producto o servicio, y además de ofreciendo algo a mayores que otros no ofrecen. El correo se debe hacer atractivo tanto visualmente como de contenido, personalizado y original. Es importante en este marketing n ofrecer fechas de ofertas[1].

Dicha base de datos debe someterse a las disposiciones legales vigentes en cuanto al manejo de la información

El email marketing es una forma de marketing online que utiliza el email como medio de comunicación entre una parte emisora (el remitente) y 2 o más receptores (los suscriptores). El email es utilizado para enviar un mensaje a los receptores, que puede ser, entre otros:

1. Promocional o de venta

2. Informativo

3. De contacto

Tenemos que ver una diferencia entre Email marketing vs email masivo y ella es el aporte de valor del primero, reduciéndose el segundo a la remisión de información. Es decir, podemos utilizar una campaña de email como un medio de comunicación directo entre nosotros, nuestra empresa, y una lista de suscriptores, clientes, o contactos, que van a recibir nuestro mensaje (email). En definitiva es una herramienta de comunicación que nos va a permitir hacer llegar nuestro mensaje, sea del tipo que sea, a nuestro público objetivo.

v. CORREO ELECTRÓNICO SENA

La Resolución No. 2159 de 2013, por la cual se cree el marco de gobierno TIC y se fijan políticos institucionales para el uso y comportamiento frene a los recursos y servicios de las TIC en la entidad; dispone en sus anexos:

[…]5. CORREO ELECTRÓNICO INSTITUCIONAL.

a) La utilización de la cuenta de correo electrónico debe tener fines estrictamente relacionados con las actividades propias del cargo, la actividad que se desempeña en la Entidad, para el estricto cumplimiento de sus funciones o del objeto de su contrato. Por tratarse de un servicio financiado con recursos públicos, el correo electrónico institucional no podrá ser utilizado por terceros.

b) El correo electrónico solo podrá ser utilizado por personal vinculado a la Entidad, sean servidores públicos o contratistas según sea el caso, y por los aprendices vinculados a la Institución.

c) Un usuario SENA tendrá máximo una cuenta de correo institucional la cual es personal e intransferible. Una dirección electrónica con los siguientes formatos: nombre-usuario@sena.edu.co para funcionarios del SENA; y nombre-usuario.ext@sena.edu.co para contratistas directos. Para la asignación del nombre de buzón se tendrán en cuenta las siguientes condiciones:

i. Se tomará la inicial del primer nombre y el primer apellido completo del usuario.

ii. En caso que ya exista esa cuenta de correo, se adicionara la inicial del segundo nombre (si lo tiene). De no tener segundo nombre, se incluirá la inicial del segundo apellido.

iii. Si ya existe este nombre de usuario, se adicionará el segundo apellido.

iv. De no ser procedentes ninguna de las formas anteriores, se conformará con el nombre completo del usuario (sin espacios).

d) Al usuario le será asignada una contraseña inicial para acceder de forma privada a su cuenta, la cual debe cambiar inmediatamente en su primer acceso. La contraseña deberá ser cambiada periódicamente según se informe mediante circular que aparecerá en el Web-Site de la Oficina de Sistemas de la Dirección General y no revelarse o compartirse con terceros. La longitud mínima de caracteres, y la conformación de caracteres de la contraseña se informará mediante

circular y aparecerá en el Web-Site de la Oficina de Sistemas de la Dirección General.

e) Todo mensaje enviado desde una cuenta de correo electrónico es responsabilidad individual del titular de la cuenta.

f) Todos los mensajes enviados deben contener los datos del usuario remitente, según las instrucciones definidas para la firma de correo electrónico, de acuerdo con el Manual de Identidad Corporativa (Res. 00334 de febrero 29 de 2012).

g) La asignación de buzones para almacenar mensajes en la infraestructura central de correo electrónico se realizará de acuerdo con tipos de usuario: Estándar, Avanzado y V.l.P. Los tamaños dispuestos para cada tipo de usuario se informará mediante circular y aparecerá en el Web-Site de la Oficina de Sistemas de la Dirección General. Dado que en cualquier caso la capacidad de almacenamiento del buzón de correo es limitada, es necesario que los usuarios realicen mantenimiento del mismo, eliminando los correos que considere requeridos para su gestión.

h) El tamaño máximo de un mensaje, incluyendo sus archivos adjuntos, tanto para envío como para recepción se informará mediante circular y aparecerá en el Web-Site de la Oficina de Sistemas de la Dirección General. En casos excepcionales, la Oficina de Sistemas de la Dirección General podrá otorgar permisos para superar este límite, previa autorización del superior de la dependencia.

i) El límite máximo de envío estándar de mensajes es a 30 destinatarios, en casos excepcionales, la Oficina de Sistemas de la Dirección General podrá otorgar permisos para superar este límite, previa autorización de (Directores Regionales, Subdirectores de Centro de Formación Profesional Integral y Secretaría General). No se permite el envío de correos masivos con archivos adjuntos de gran tamaño que puedan congestionar la red. El tamaño máximo del correo masivo interno para el SENA se indica en el Anexo Técnico de esta Resolución, que se encuentre vigente.

j) Las cuentas autorizadas a emitir mensajes masivos a más de 30 destinatarios son exclusivos para Dirección General, Oficina de Comunicaciones y Oficina de Sistemas. Para los usuarios de otras áreas que necesiten emitir mensajes masivos a más de 30 destinatarios harán lo siguiente dependiendo de la frecuencia de los mensajes:

- con baja frecuencia, deberán dirigirse a la Oficina de Comunicaciones para su emisión. Se entiende por baja frecuencia hasta un mensaje a la semana.

- con alta frecuencia (más de un mensaje semanal y durante varias semanas), deberán recurrir a la Oficina de Comunicaciones para crear un sitio Web en la Intranet para hacer la publicación de su información; y los mensajes que emitan desde estas cuentas tendrán una breve descripción y el vínculo a la dirección URL donde está la información que se desea revelar. El contenido de la información de los sitios Web es responsabilidad única del líder del proyecto o grupo especial, debe cumplir las políticas descritas en el presente literal y debe tener la advertencia de que su contenido no representa la posición oficial del SENA.

PARAGRAFO. A partir de la publicación de la presente resolución quedarán suspendidas todas las cuentas de manejo de correos masivos, a excepción de las especificadas en este literal. Los usuarios que quieran hacer uso de este servicio desde otras fuentes deben solicitar su registro utilizando el mecanismo que al efecto defina la Oficina de sistemas de la Dirección General.

k) Las cuentas para proyectos o grupos especiales (cuentas genéricas), se crearán exclusivamente por solicitud del autorizador (Directores Regionales, Subdirectores de Centro de Formación Profesional Integral y Secretaría General) y deben ser asignadas a un único responsable para su gestión.

l) La información transmitida por medio del correo electrónico Institucional es considerada información oficial y debe ser manejada confidencialmente entre el remitente y los destinatarios.

m) La cuenta de correo electrónico institucional asignada por el SENA, debe ser utilizada para atender los asuntos oficiales de la entidad.

n) Los correos electrónicos deben contener la sentencia de confidencialidad con el siguiente contenido: "CONFIDENCIALIDAD: Este correo electrónico es correspondencia j confidencial del SENA. Si Usted no es el destinatario correcto, le solicitamos informe inmediatamente al correo electrónico del remitente; así mismo, por favor bórrelo y por ningún motivo haga público su contenido; de hacerlo, la divulgación podrá acarrear acciones legales. Si Usted es el destinatario, le solicitamos observar absoluta reserva sobre el contenido, los datos e información de contacto del remitente, o la de aquellos a quienes les enviamos copia, y en general sobre la información incluida en este documento o archivos adjuntos, a menos que exista una autorización explícita a su nombre."

o) Está prohibido sustituir la identidad de otro usuario de un sistema de comunicaciones electrónicas del SENA.

p) En ningún caso la información oficial que la Institución envíe al personal mediante correo electrónico, podrá ser clasificada como correo no deseado.

q) No se permite el envío de correos SPAM (correo no deseado), con contenido que resulte molesto o dañino para los usuarios del servicio, o que atente contra la integridad de las personas o instituciones, tales como: material pornográfico, chistes, temas religiosos, racistas, políticos, terrorismo y cualquier contenido que represente riesgo de propagación de virus informáticos.

r) El correo institucional no podrá ser utilizado en forma nociva para realizar acoso, calumnias, difamación o para divulgar contenidos que pretendan intimidar, insultar o realizar cualquier otra forma de actividad hostil, en contra de los funcionarios, las instituciones o el público en general.

s) No se podrá utilizar el correo electrónico para reemplazar procedimientos administrativos y de gestión, que hayan sido previamente establecidos al interior de la Entidad y que deban agotar un trámite diferente.

t) Se prohíbe el envío de mensajes a través de direcciones de correo diferentes a la asignada, así como la lectura, modificación o eliminación de mensajes enviados a otras cuentas, sin autorización expresa de su titular.

u) Se prohíbe el envío de software, música en cualquier formato, bases de datos, imágenes, fotografías o archivos similares, cuyo uso transgreda las disposiciones de la presente resolución, y lo enunciado al respecto en la legislación supranacional y nacional sobre propiedad intelectual y derechos de autor.

v) La Subdirección de Recursos Humanos y Grupo de Contratación son los responsables de solicitar la creación, modificación o cancelación de las cuentas electrónicas a la Mesa de

Servicios. (Subraya fuera de texto)

Ahora bien la misma normativa dispone frente al correo electrónico de los aprendices SENA, lo siguiente:

[…] 4. CORREO ELECTRÓNICO.

a) Un aprendiz podrá tener máximo una cuenta de correo en el SENA.

b) El uso del correo debe ser utilizado solamente para propósitos educativos y de investigación.

c) Le será provista una contraseña inicial para acceder de forma privada a su cuenta, la cual debe cambiar inmediatamente en su primer acceso. La contraseña deberá ser cambiada periódicamente. Y no debe revelarse o compartir su contraseña con terceros o hacerse pasar por otra persona. La longitud mínima de caracteres, y la conformación de caracteres de la contraseña se informará mediante circular y aparecerá en el Web-Site de la Oficina de Sistemas de la Dirección General.

d) El tamaño del buzón de correo electrónico se informará mediante circular y aparecerá en el Web-Site de la Oficina de Sistemas de la Dirección General.

e) Los aprendices del SENA, podrán solicitar la ampliación de la capacidad máxima de su buzón que se indica en el Anexo Técnico de esta Resolución, por intermedio del Subdirector de Centro de Formación Profesional Integral, respectivo.

f) Todo mensaje enviado desde una cuenta de correo electrónico es responsabilidad individual del titular de la cuenta.

g) En el uso del correo electrónico, no revelar información personal, como su dirección y número telefónico.

h) El contenido de una cuenta de directorio de red son responsabilidad individual del titular de la cuenta.

i) Los aprendices no deben usar correo electrónico del SENA, para obtener o enviar material que esté en contra de la ley o las normas institucionales publicados (artículos que sexistas, racistas, obscenos, políticos o que promueva conductas ilegales).

j) Los aprendices deben abstenerse de enviar o mostrar mensajes o imágenes ofensivas.

k) Las revisiones de rutina de las áreas de almacenamiento de red se llevarán a cabo sin previo aviso.

l) Se recomienda a los aprendices que ante un fallo de seguridad informen a un miembro del personal autorizado del SENA y asegurar que las contraseñas se cambian con el fin de ser lo más seguro posible.

m) No debe traer intencionalmente virus; materiales o aplicaciones protegidas derechos de autor en el SENA. (Subraya fuera de texto)

De lo anterior podemos concluir que el uso del correo electrónico institucional se enmarca dentro de las actividades institucionales y oficiales del SENA, así quienes tienen un vínculo con la entidad no pueden utilizarlo para fines diferentes. Así mismo puede ser emisor y receptor de

mensajes, algunos calificados como masivos o colectivos, estos sometidos a una reglamentación especial, herramienta que no todos pueden utilizar.

En consecuencia y frente al mailing el correo es la herramienta a través de la cual se realiza el envío de la información, folleto o carta personalizada, con fines informativos, promocionales o de contacto.

a) CONCLUSIONES

-Los datos personales contenidos en una base de datos susceptible de tratamiento por una persona pública o privada son susceptibles de protección por la Constitución Política (artículos 15 y 209 y la Ley 1581 de 2012. Por lo anterior debe tenerse presente:

- La autorización, se entiende como el consentimiento previo, expreso e informado del titular de la información para el manejo de la misma.

- Base de datos es el conjunto organizado de datos personales objeto de trato.

- El titular es la persona natural cuyos datos son objeto de tratamiento.

- Tratamiento es la operación u operaciones sobre los datos personales, incluye recolección, uso, circulación, supresión, almacenamiento.

- El tratamiento de datos obedece a una finalidad legítima,

- La información relacionada con datos de menores-adolescentes, tiene un tratamiento preferencial según lo dispuesto en la Ley 1581 de 2012, artículo 7; donde solo se permite el tratamiento de datos de naturaleza pública. El Estado, entiéndase el SENA como integrante de su estructura a nivel nacional, debe evitar el uso inadecuado de los datos personales de los menores de 18 años. Los servidores públicos deben proteger los derechos derivados del uso de los datos personales de los menores de 8 años.

- El correo electrónico es la herramienta más utilizada para el envío del mailing. El mailing es un tipo de marketing directo que puede ser para uso informativo, promocional, de venta, o de contacto. Señalan que es diferente email marketing y email masivo este último que se restringe al tema de remisión de información.

- Si el correo electrónico utilizado es institucional, entonces la información transmitida por medio del correo electrónico Institucional es tratada como información oficial y debe ser manejada confidencialmente entre el remitente y los destinatarios; así mismo la cuenta de correo electrónico institucional asignada por el SENA, debe ser utilizada, por quienes tienen vínculo vigente (servidores, aprendices y contratistas) para atender los asuntos oficiales de la entidad.

- En este orden de ideas, los mailing (marketing directos) enviados por el correo institucional de la entidad, que contengan información o promoción, masiva o de contacto, referida a los propósitos educativos y de investigación, y en general del giro ordinario de la misión del SENA; y además, no involucren datos sensibles, información reservada y en general el derecho a la intimidad, no necesitan autorización o que se levante ninguna reserva. Lo anterior, no sin advertir la necesidad de atender los parámetros relacionados con los derechos de propiedad intelectual y derechos de autor en cada caso particular.

- Ahora bien la base de datos soporte para el uso de este tipo de email marketing debe respetar

todas las normas relacionadas con tratamiento de la información ya analizada.

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.

Cordialmente,

Carlos Emilio Burbano Barrera

Coordinador

<NOTAS DE PIE DE PÁGINA>.

1. https://www.gestion.org/que-es-el-mailing/

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)