CONCEPTO 26163 DE 2018

<Fuente: Archivo interno entidad emisora>

SERVICIO NACIONAL DE APRENDIZAJE - SENA

PARA:	Juan Felipe Rendón Ochoa - Director Regional Antioquia- SENA jrendon@sena.edu.co
DE:	Coordinador Grupo de Conceptos Jurídicos y Producción Normativa
ASUNTO:	Correo institucional/Copias de seguridad/Copias de respaldo/Backup

En atención a su solicitud remitida por correo electrónico de fecha 07 de mayo del año en curso, radicado 8- 2018- 023913, oportunidad en la cual solicita concepto respecto de la normatividad que permita o prohíba la realización de copia de seguridad o Backup de la información de los correos electrónicos institucionales y del software que reposa en los computadores asignados tanto de contratistas como de funcionarios; 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.

De manera comedida le informo que esta dependencia no es la competente para resolver situaciones particulares ni conceptuar sobre procedimientos de trámites o hacer aclaraciones/modificaciones a los actos administrativos proferidos por el SENA, motivo por el cual las consultas se abordan en forma general.

CONCEPTO JURÍDICO

a. ANTECEDENTES

Señala quien consulta:

- A los contratistas y funcionarios se les asigna un correo electrónico institucional y un computador de propiedad del SENA, para permitir y facilitar el desarrollo de su objeto contractual o de sus funciones, están obligados contratistas y funcionarios a utilizar el correo electrónico institucional y computador asignado única y exclusivamente para los fines relacionados con su objeto contractual o funciones o podrían utilizar estos recursos para algunos asuntos personales.

- Gozarían contratistas y funcionarios de derechos fundamentales como el de la intimidad, el de protección de datos personales (hábeas data) y el de inviolabilidad de la correspondencia y demás formas de comunicación respecto del correo electrónico institucional y del computador asignado.

- Existe presunción de privacidad frente al correo, el computador y demás formas de comunicación que usa el contratista y funcionario.

- En caso de existir presunción de privacidad, es necesario que el contratista o funcionario tenga conocimiento previo e informado que el correo, el computador y demás formas de comunicación

son de carácter institucional, para desvirtuar tal presunción, cuál es el documento donde reposa esa información tanto para contratistas como para funcionarios.

- Existe en el SENA una política o reglamento sobre las normas para el uso de los servicios de tecnologías de información y telecomunicaciones y recursos informáticos, tanto para contratistas como para funcionarios

- Se considera una herramienta de trabajo el correo electrónico institucional y el computador de propiedad del SENA y por ende es posible exigir al contratista y al funcionario efectuar un Back Up de ello y cuál sería el mecanismo para exigir al funcionario y/o contratista dicha información.

- De considerarse una herramienta de trabajo puede en cualquier momento y circunstancia el empleador o el supervisor del contrato realizar copia de seguridad o Back Up sin previa autorización del funcionario o contratista y toda la información que allí repose se considera de propiedad intelectual del SENA o cuál sería el protocolo para realizar dicho procedimiento.

- Se solicita concepto respecto de la normatividad que permita o prohíba la realización de copia de seguridad o Back Up de la información de los correos electrónicos institucionales y del software que reposa en los computadores asignados tanto de contratistas como de funcionarios así como quien sería la persona autorizada para ello.

(Subraya fuera de texto, para resaltar los interrogantes planteados)

- Se deja constancia que la consulta se absuelve con la información suministrada.

b. ANÁLISIS

i. SENA/POLÍTICA O REGLAMENTO TECNOLOGÍAS DE LA INFORMACIÓN Y TELECOMLUNICACIONES Y RECURSOS INFORMÁTICOS.

El SENA dentro de los lineamientos estratégicos tiene como uno de sus objetivos, fortalecer la gestión de la infraestructura física y tecnológica de la entidad. Además, tiene sus estrategias, “fomentar la cultura del uso de las TIC, para ofrecer sentidos transparentes y de mayor calidad con posibilidad de interoperabilidad entre dependencias a través de conexiones rápidas y seguras”.

De otra parte, y en concordancia con el numeral 4 del artículo 8 del Decreto 249 de 2004, establece que es función de la Oficina de Sistemas: “Asesorar a las dependencias de la entidad en la aplicación de políticas, estrategias y directrices trazadas por la Dirección General, relacionadas con el desarrollo informático de la entidad y en la ejecución de los planes correspondientes”. En el mismo sentido, el artículo 8 del Decreto 249 en cita, establece que la Oficina de Sistemas tiene entre otras las siguientes funciones:

- Asistir a la Dirección General y a las demás dependencias del SENA, en la implementación de los sistemas, normas y procedimientos de informática requeridos por la entidad.

- Asesorar a las dependencias de la entidad en la aplicación de las políticas, estrategias y directrices trazadas por la Dirección General, relacionadas con el desarrollo informático de la entidad y en la ejecución de los planes correspondientes.

- Conceptuar, evaluar y definir las necesidades y lineamientos para la adquisición, adaptación, desarrollo de bienes, custodia, mantenimiento, administración de contingencias y actualización

de las plataformas y de los bienes informáticos en la Entidad, en coordinación con la Dirección Administrativa y Financiera y con las áreas usuarias del SENA.

- Coordinar con la Secretaría General, las directrices y orientaciones para la elaboración de planes de capacitación en informática para los funcionarios de la entidad.

El Decreto 2482 de 2012, "por el cual se establecen los lineamientos generales para la integración de la planeación y la gestión", tiene por objeto adoptar el modelo integrado de planeación y gestión como instrumento de articulación y reporte de planeación, el cual comprende entre otros, las políticas de desarrollo administrativo, las cuales comprenden el aprovechamiento del talento humano y el uso eficiente de los recursos administrativos, financieros y tecnológicos.

El referido Decreto 2482 de 2012, advierte en su artículo 6, que la instancia responsable a nivel institucional para liderar, coordinar y facilitar la implementación del modelo integrado de planeación y gestión, es el Comité Institucional de Desarrollo Administrativo y que este Comité sustituirá los demás comités que tengan relación con el modelo y no sean obligatorios por mandato legal. En consecuencia, mediante la Resolución 646 de 2013, se crea el Comité Institucional de Desarrollo Administrativo del Servicio Nacional de Aprendizaje SENA.

El anterior Comité establece dentro de sus funciones: "[...] 14. Determinar los mecanismos para implementar la normatividad relacionada con la estrategia de Gobierno en línea. 15. Definir los lineamientos para la implementación efectiva de políticas y estándares asociados como la política de actualización del sitio web, política de uso aceptable de la red y de internet, política de servicios por medios electrónicos, política de privacidad y condiciones de uso y política de seguridad del sitio web, entre otros".

En este contexto de las TIC's se han emitido a nivel nacional, dentro de las principales, las siguientes normas:

- La Ley 1341 de 2009, que define principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones - TIC. masificación del Gobierno en Línea, etc.

- La Ley 1450 de 2011, por la cual se expide el Plan Nacional de Desarrollo 2010- 2014, que plantea el Gobierno en Línea como Estrategia de Buen Gobierno. (Artículo 230)

- El Decreto 1151 de 2008, Decreto 2693 de 2012. Normatividad que establece los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente las Leyes 962 de 2005, 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

- Manual vigente GEL, para la implementación de la Estrategia de Gobierno en línea Entidades del Orden Nacional, permitiendo en la Entidad el fortalecimiento en Gestión de Seguridad de TI y de la Información, eficiencia administrativa y lineamientos de la política de Cero Papel, racionalización de trámites y procesos administrativos, fortalecimiento tecnológico y habeas data.

- Ley 527 de 1999, define y reglamenta el uso y acceso a los mensajes de datos, determinando su naturaleza, requisitos y forma de comunicación en las entidades estatales.

- Derechos de autor, la entidad propenderá por el respeto y cumplimiento de las buenas prácticas, sin vulnerar la propiedad intelectual como lo dispone la Ley 23 de 1982, la Directiva Presidencial 01 de 1999, la Directiva Presidencial 02 de 2002, y las Circulares de la Dirección Nacional de Derechos de Autor Nos. 04 de 2006, 12 de 2007 y 17.

En este orden de ideas, las instalaciones del SENA, cuentan con la presencia de recursos y servicios de Tecnologías de las Información y las Comunicaciones (TIC), los cuales son esenciales para el normal funcionamiento de la entidad. Igualmente, las tecnologías de la información para la enseñanza y el aprendizaje (e- leaming) deben ser apropiadas adecuadamente por parte de los instructores y personal de apoyo para innovar en enseñanza y aprendizaje, generando contenido para la formación efectiva de aprendices y la capacitación del personal del SENA.

En consecuencia, fue necesario fomentar la cultura de racionalización de los recursos y servicios TIC del SENA, de acuerdo con las normas vigentes que regulan la protección de los recursos públicos y las recomendaciones para un uso de las TIC ecológica y sostenible (Green IT). Es así como fue expedida por el SENA la Resolución No. 2159 de 2013, "por la cual se crea el Marco de Gobierno TIC y se fijan Políticas Institucionales para el uso y comportamiento frente a los recursos y servicios de las TIC por parte de los usuarios internos del SENA", la cual dispuso en su anexo No. 1 las "POLÍTICAS TIC PARA FUNCIONARIOS Y CONTRATISTAS".

En consecuencia, dispone el acto administrativo en comento, en sus artículos 1 y 2 lo siguiente:

ARTÍCULO PRIMERO. OBJETIVO. Crear el Marco de Gobierno de las Tecnologías de la Información y Comunicaciones en el SENA, mediante la definición de las Políticas Institucionales para la adquisición, desarrollo y el uso de los recursos y servicios de las TIC en la Entidad.

ARTÍCULO SEGUNDO. ALCANCE. Las Políticas institucionales contempladas en esta Resolución, establecen las responsabilidades de las personas (funcionarios y contratistas del SENA y aprendices) que hacen uso de los recursos y servicios de las TIC, dispuestos por la entidad para el cumplimiento de sus funciones, el logro de la misión y los objetivos institucionales, de acuerdo con las Leyes y la normatividad vigente. (Subraya fuera de texto)

El artículo 3 de la Resolución en comento, establece que la Oficina de Sistemas de la Dirección General es responsable de definir, desarrollar y evaluar estrategias, políticas, procedimientos, manuales, instructivos y recomendaciones, relacionadas con la gestión de los recursos y servicios de las TIC las cuales deben estar alineadas con el plan estratégico de desarrollo de la entidad. Por lo tanto, todas las actividades concernientes a la aprobación, adquisición, instalación, configuración, liberación, mantenimiento, soporte, baja, traslado, distribución, control y monitoreo de los recursos y servicios de las TIC, deben estar coordinadas por esta Oficina.

En concordancia con lo anterior, en el artículo 5 dispone la multicitada resolución, que "[…] sin detrimento de la facultad de administración, monitoreo y control que ejerce la Oficina de Sistemas de la Dirección General, sobre las actividades relativas al uso de los recursos y servicios de las TIC de la entidad, los Directores de Área, Jefes de Oficina, Directores Regionales y Subdirectores de Centro de Formación Profesional Integral, deberán adoptar medidas tendientes a garantizar el cumplimiento por parte de las personas a su cargo, de las responsabilidades descritas en la presente Resolución, con el objeto de evitar que se incurra en acciones lesivas a los intereses de la entidad". (Subraya fuera de texto)

Dentro de las políticas fijadas se consideran dos tipos de usuarios: los funcionarios y contratistas ambos del SENA, así como los aprendices, los cuales deben cumplir con políticas específicas. Así se estableció:

Anexo 1. Las políticas de TIC que deben cumplir los funcionarios y contratistas del SENA, las cuales están divididas por tipo de servicios TIC o temas relacionados, como se relacionan a continuación;

- Gestión de usuarios	- Servicio de acceso remoto
- Mesa de servicios	- Móviles personales
- Activos de información	- Videoconferencia
- Sistema de información	- Green IT
- Correo electrónico institucional	- Adquisición de elementos TIC
- Internet	- Donaciones
- Redes de comunicaciones	- Energía y centros de cableado

Anexo 2. Las políticas de TIC que deben cumplir los aprendices del SENA, las cuales están divididas por tipo de servicios TIC o temas relacionados, como se relacionan a continuación:

- Gestión de Usuarios	- Equipo TIC
- Internet	- Dispositivos Móviles
- Correo Electrónico	

Es oportuno señalar, que a través de la Resolución No. 219 de 2013, que derogó la Resolución No. 334 de 2012, “por la cual se adopta el Protocolo de Comunicaciones del SENA y se deroga la Resolución No 0334 de 2012", se señaló, entre otros, que el protocolo de comunicaciones del SENA está constituido por los siguientes Manuales:

1. Manual de Comunicaciones. Guía que orienta las actuaciones públicas de los servidores públicos del SENA.

2. Manual de Identidad Corporativa. Establece los parámetros para la utilización pública de la imagen de la Entidad.

3. Manual de Páginas Electrónicas y Redes Sociales. Fija las pautas para la utilización y acceso a nombre de la Entidad, a las páginas electrónicas oficiales, blogs y cuentas en redes sociales.

4. Manual de Eventos. Es una guía para la preparación de los eventos y la utilización de la imagen institucional en los mismos.

El tercer manual, contiene todo lo relacionado con el correo electrónico, el portal web, el blogs, la intranet y las redes sociales del SENA.

ii. USO DE COMPUTADORES/EQUIPOS DE CÓMPUTO POR SERVIDORES PUBLICOS Y CONTRATISTAS

Dado el fin y lo que comprende el uso del computador o equipo de cómputo como herramienta para el cumplimiento de las funciones o de los objetos contractuales por parte de servidores públicos y contratistas, el cual permite entre otros, la elaboración de documentos, el acceso a internet, correo electrónico, redes sociales, etc.; lo que involucra el uso de recursos y servicios de

las TIC dispuestos por el SENA; la entidad mediante la Resolución No. 2159 de 2013, dispuso que tanto funcionarios (servidores públicos) como contratistas responden por el buen o mal uso de dicha herramienta.

También dicha resolución determina en su artículo 6, que es responsabilidad de todos los funcionarios o contratistas del SENA que hacen uso de los recursos y servicios de las TIC poner en conocimiento de la Oficina de Control Interno Disciplinario, cualquier incumplimiento a las Políticas definidas en la referida Resolución y a las normas vigentes. Igualmente, se establece, como los servidores y contratistas del SENA para el cumplimiento de sus funciones y obligaciones contractuales, el logro de la misión y los objetivos institucionales, deben hacer uso exclusivo de las herramientas destinadas y autorizadas para el acceso a Internet que suministra la entidad.

Finalmente, también señala la entidad, que está prohibido descargar y almacenar archivos en MP3, fotografías videos, imágenes de cualquier naturaleza, presentaciones en PowerPoint, etc., en los medios de almacenamiento del computador asignado, cuando estos contenidos no estén relacionados con las funciones o actividades del cargo desempeñado.

En concordancia con lo anterior, frente a los servidores públicos es oportuno señalar lo dispuesto por la Ley 734 de 2004- Código Disciplinario Único:

ARTÍCULO 34. Deberes. Son deberes de todo servidor público:

1. Cumplir y hacer que se cumplan los deberes contenidos en la Constitución, los tratados de Derecho Internacional Humanitario, los demás ratificados por el Congreso, las leyes, los decretos, las ordenanzas, los acuerdos distritales y municipales, los estatutos de la entidad, los reglamentos y los manuales de funciones, las decisiones judiciales y disciplinarias, las convenciones colectivas, los contratos de trabajo y las órdenes superiores emitidas por funcionario competente.

Los deberes consignados en la Ley 190 de 1995 se integrarán a este código.

[…]

4. Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos.

5. Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos.

[…]

11. Dedicar la totalidad del tiempo reglamentario de trabajo al desempeño de las funciones encomendadas, salvo las excepciones legales.

[…]

21. Vigilar y salvaguardar los bienes y valores que le han sido encomendados y cuidar que sean utilizados debida y racionalmente, de conformidad con los fines a que han sido destinados.

22. Responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización. (Subraya fuera de texto)

A su turno la norma precitada establece:

ARTÍCULO 35. Prohibiciones. A todo servidor público le está prohibido:

1. Incumplir los deberes o abusar de los derechos o extralimitar las funciones contenidas en la Constitución, los tratados internacionales ratificados por el Congreso, las leyes, los decretos, las ordenanzas, los acuerdos distritales y municipales, los estatutos de la entidad, los reglamentos y los manuales de funciones, las decisiones judiciales y disciplinarias, las convenciones colectivas y los contratos de trabajo.

[…]

13. Ocasionar daño o dar lugar a la pérdida de bienes, elementos, expedientes o documentos que hayan llegado a su poder por razón de sus funciones. (Subraya fuera de texto)

En conclusión, no cabe duda alguna que las herramientas entregadas para cumplir con las funciones asignadas, como es el caso del computador, tanto en el caso de servidores públicos como en el de los contratistas, tiene uso exclusivo para la labor asignada y es propiedad de la entidad estatal en su calidad de empleadora o de contratante.

iii. SENA/CORREO ELECTRÓNICO INSTITUCIONAL

El correo electrónico es un nuevo medio de comunicación que permite la transmisión de datos, el flujo o distribución de material protegido por el derecho de autor, transacciones económicas y correspondencia en general. Este servicio de Internet se define de la siguiente forma: "El correo electrónico constituye un servicio de mensajería electrónica que tiene por objeto la comunicación no interactiva de texto, datos, imágenes o mensajes de voz entre un "originador" y los destinatarios designados y que se desarrolla en sistemas que utilizan equipos informáticos y enlaces de telecomunicaciones".[1]

Este correo hace las veces de una comunicación o carta, también corresponde a un conjunto de datos del usuario, los cuales pueden estar en la órbita de la privacidad del mismo, y finalmente a través de él pueden transmitirse textos protegidos desde la órbita de los derechos de autor; en cada escenario, se protegerán los datos conforme con la normatividad vigente, y considerando, lo reglamentado por cada entidad en el caso de correos institucionales.

Así al permitir el trasegar de documentos en formato de texto, imagen o sonido, e incluso archivos multimediales, el correo electrónico se ha constituido en una herramienta de difusión de material protegido por el derecho de autor. Por su parte el Ministerio de las Telecomunicaciones ha señalado que el correo electrónico es una herramienta para el intercambio de información entre personas, no es una herramienta de difusión de información masiva tipo spam o cadenas[2].

En este orden de ideas, se establece como parámetro en la gestión documental del SENA, la seguridad de la información, entendida como el conjunto de medidas preventivas que permiten proteger la información, buscando mantener la confidencialidad, la disponibilidad y la integridad de la misma.

Las políticas específicas fijadas en los anexos del acto administrativo proferido establecen el buen uso de los recursos y servicios de las Tecnologías de la Información y Comunicaciones

(TIC) del SENA que deben cumplir todas las personas y dependencias de la Entidad a nivel nacional. Así dentro de las políticas TIC para funcionarios y contratistas del SENA, el numeral 5 anexo a la Resolución No. 2159 de 2013, se encuentra lo relacionado al correo institucional, así:

[…] 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 (Resolución No. 00334 (*0034) de febrero 29 de 2012, derogada por la Resolución No. 219 de 2013).

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 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 y negrilla fuera de texto)

De lo anterior podemos concluir, que el uso del correo es solamente para asuntos oficiales de la entidad, además que la información que a través de él se transmite es la oficial, del SENA en ejercicio de sus funciones y de su propiedad, y se maneja con la confidencialidad requerida y regulada por la normatividad vigente. Así, se restringe su uso para aspectos personales o fines diferentes a los institucionales.

En cuanto a los sistemas de información se advierte que en el SENA:

[…] 4. SISTEMAS DE INFORMACIÓN.

a) El usuario será responsable del uso y mantenimiento que haga de su cuenta y control de acceso en los sistemas de información, so pena de incurrir en una denuncia penal por mal uso de los

servicios informáticos de la entidad.

b) El usuario deber proteger su equipo de trabajo, evitando que personas ajenas a su cargo puedan acceder a la información almacenada en él, mediante una herramienta de bloqueo temporal (protector de pantalla), protegida por una contraseña, la cual debe activarse en el preciso momento en que el usuario deba ausentarse.

c) El usuario es responsable de eliminar cualquier rastro de documentos proporcionados por el Administrador de la red, que contenga información que pueda facilitar a un tercero la obtención de la información de su cuenta de usuario. […] (Subraya fuera de texto)

Igualmente, el documento emitido por el SENA, trata de manera independiente y clara el tema de la responsabilidad frente a los correos electrónicos:

[…] 5.2 RESPONSABILIDADES FRENTE AL CORREO ELECTRÓNICO INSTITUCIONAL.

Es responsabilidad de todos los usuarios del correo institucional:

a) Revisar periódicamente el correo electrónico.

b) Depurar frecuentemente el contenido del buzón de correo para evitar que los mensajes permanezcan en éste un tiempo excesivo, que derive en la congestión o bloqueo del mismo.

c) Mantener reserva sobre las claves de acceso al computador y al sistema de correo electrónico institucional, aplicando las políticas de cambio de clave establecidas.

d) Realizar mensualmente copias de respaldo de sus archivos y de sus carpetas de mensajes de correo en el computador asignado para el cumplimiento de labores en la Entidad. Se entenderá que el contenido del buzón de correo está integrado por archivos en tránsito y no almacenados en forma permanente. Cada usuario es responsable de la actualización de dichas copias. Se debe enviar un manual para usuario el cual indique el proceso.

e) Conservar activo y actualizado en el computador el software de protección contra virus que revise el contenido de los mensajes entrantes y salientes del correo. Esta actualización se hará por lo menos una vez a la semana, teniendo en cuenta que después de instalado el programa será de entera responsabilidad del usuario verificar y atender las alertas que se generen.

f) Utilizar lenguaje adecuado en cada una de las comunicaciones que sean enviadas tanto al interior de la Entidad como a otras entidades, o al público en general, observando normas de carácter ético y de respeto por las personas.

g) No suministrar el nombre de la cuenta de correo a personal no confiable, ni inscribirla en listas de correo externo, cadenas o páginas comerciales. (Subraya fuera de texto)

iv. PROTECCIÓN DE DATOS PERSONALES/HABEAS DATA

a. 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", reza en cuanto a su ámbito de aplicación:

ARTÍCULO 2. Ámbito de aplicación. La presente ley se aplica a todos los datos de información personal registrados en un banco de datos, sean estos administrados por entidades de naturaleza pública o privada.

Esta ley se aplicará sin perjuicio de normas especiales que disponen la confidencialidad o reserva de ciertos datos o información registrada en bancos de datos de naturaleza pública, para fines estadísticos, de investigación o sanción de delitos o para garantizar el orden público.

Se exceptúan de esta ley las bases de datos que tienen por finalidad producir la Inteligencia de Estado por parte del Departamento Administrativo de Seguridad, DAS, y de la Fuerza Pública para garantizar la seguridad nacional interna y externa.

Los registros públicos a cargo de las cámaras de comercio se regirán exclusivamente por las normas y principios consagrados en las normas especiales que las regulan.

Igualmente, quedan excluidos de la aplicación de la presente ley aquellos datos mantenidos en un ámbito exclusivamente personal o doméstico y aquellos que circulan internamente, esto es, que no se suministran a otras personas jurídicas o naturales.

En el mismo sentido, el legislador en la norma precitada, estableció principios que rigen el manejo de la información en bases de datos:

ARTÍCULO 4. Principios de la administración de datos. En el desarrollo, interpretación y aplicación de la presente ley, se tendrán en cuenta, de manera armónica e integral, los principios que a continuación se establecen:

a) Principio de veracidad o calidad de los registros o datos. La información contenida en los bancos de datos debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el registro y divulgación de datos parciales, incompletos, fraccionados o que induzcan a error;

b) Principio de finalidad. La administración de datos personales debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley. La finalidad debe informársele al titular de la información previa o concomitantemente con el otorgamiento de la autorización, cuando ella sea necesaria o en general siempre que el titular solicite información al respecto;

c) Principio de circulación restringida. La administración de datos personales se sujeta a los límites que se derivan de la naturaleza de los datos, de las disposiciones de la presente ley y de los principios de la administración de datos personales especialmente de los principios de temporalidad de la información y la finalidad del banco de datos.

Los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la presente ley;

d) Principio de temporalidad de la información. La información del titular no podrá ser suministrada a usuarios o terceros cuando deje de servir para la finalidad del banco de datos;

e) Principio de interpretación integral de derechos constitucionales. La presente ley se interpretará en el sentido de que se amparen adecuadamente los derechos constitucionales, como son el hábeas data, el derecho al buen nombre, el derecho a la honra, el derecho a la intimidad y el derecho a la información. Los derechos de los titulares se interpretarán en armonía y en un plano de equilibrio con el derecho a la información previsto en el artículo 20 de la Constitución y con los demás derechos constitucionales aplicables;

f) Principio de seguridad. La información que conforma los registros individuales constitutivos de los bancos de datos a que se refiere la ley, así como la resultante de las consultas que de ella hagan sus usuarios, se deberá manejar con las medidas técnicas que sean necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado;

g) Principio de confidencialidad. Todas las personas naturales o jurídicas que intervengan en la administración de datos personales que no tengan la naturaleza de públicos están obligadas en todo tiempo a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende la administración de datos, pudiendo sólo realizar suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

En el mismo sentido, el artículo 5 de la norma ibídem advirtió:

ARTÍCULO 5. Circulación de información. La información personal recolectada o suministrada de conformidad con lo dispuesto en la ley a los operadores que haga parte del banco de datos que

administra, podrá ser entregada de manera verbal, escrita, o puesta a disposición de las siguientes personas y en los siguientes términos:

a) A los titulares, a las personas debidamente autorizadas por estos y a sus causahabientes mediante el procedimiento de consulta previsto en la presente ley.

b) A los usuarios de la información, dentro de los parámetros de la presente ley.

c) A cualquier autoridad judicial, previa orden judicial.

d) A las entidades públicas del poder ejecutivo, cuando el conocimiento de dicha información corresponda directamente al cumplimiento de alguna de sus funciones.

e) A los órganos de control y demás dependencias de investigación disciplinaria, fiscal, o administrativa, cuando la información sea necesaria para el desarrollo de una investigación en curso.

f) A otros operadores de datos, cuando se cuente con autorización del titular, o cuando sin ser necesaria la autorización del titular el banco de datos de destino tenga la misma finalidad o una finalidad que comprenda la que tiene el operador que entrega los datos. Si el receptor de la información fuere un banco de datos extranjero, la entrega sin autorización del titular sólo podrá realizarse dejando constancia escrita de la entrega de la información y previa verificación por parte del operador de que las leyes del país respectivo o el receptor otorgan garantías suficientes para la protección de los derechos del titular.

g) A otras personas autorizadas por la ley. (Subraya fuera de texto)

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".

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 regirse conforme a 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 Estatutaria 1581 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. [3] 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

b. SENA Y MANEJO DE INFORMACIÓN

El Acuerdo No. 009 del 14 de diciembre de 2016, "por el cual se aprueba la Política del tratamiento para la Protección de Datos Personales en el Servicio Nacional de Aprendizaje (SENA)", establece que:

[…] El SENA se compromete a garantizar la protección de los derechos fundamentales referidos al buen nombre y al derecho de información, en el tratamiento de los datos personales o de cualquier otro tipo de información que sea utilizada o repose en sus bases de datos y archivos y hará uso de los mismos únicamente para los fines que se encuentra facultado, especialmente las señaladas en el título Tratamiento de la Información y Finalidad de los Datos de la presente política y sobre la base de la ley y la normatividad vigente.

En este sentido, el correo electrónico institucional hace las veces de una comunicación o carta, también corresponde a un conjunto de datos del usuario, los cuales pueden estar en la órbita de la privacidad del mismo, y finalmente, a través de él pueden transmitirse textos protegidos desde la órbita de los derechos de autor; en cada escenario, se protegerán los datos conforme con la normatividad vigente, y considerando, lo reglamentado por cada entidad en el caso de correos institucionales.

En este sentido, se entendería que los correos electrónicos de funcionarios públicos, enviados o recibidos desde su correo institucional y en ejercicio de funciones públicas - no los que tengan que ver con su vida privada o personal o que contengas este tipo de información- , se considera información oficial y es de propiedad de la entidad, salvo que se acredita la concurrencia de una causal legal específica de secreto o reserva. En este sentido la reserva o privacidad de la información depende de su contenido, eso sí considerando que estos correos deben manejar información institucional y no personal.

De acuerdo con la Resolución No. 2159 de 2013, se parte del hecho según el cual tanto los equipos y los programas instalados en ellos, así como los datos creados, almacenados y recibidos, son propiedad del SENA. Es así como se establece que en el SENA es facultad de la Oficina de Sistemas verificar el contenido de los mensajes de datos, enviados a las cuentas de correo electrónico de la entidad, por ser un servicio institucional y de su propiedad. Tal verificación se realizará cuando dicho contenido contravenga las disposiciones enunciadas, sin perjuicio del derecho constitucional a la intimidad de cada uno de los usuarios, según lo dispuesto en el artículo 15 de la Constitución Política. Respecto a la privacidad y derechos de terceros, no está permitido acceder o copiar correo electrónico, direcciones, datos, programas u

otros archivos sin permiso del titular.

v. BACKUP DE LA INFORMACIÓN

Una copia de seguridad, es un duplicado de nuestra información más importante, y la hacemos para salvaguardar los documentos, archivos, fotos, etc., de nuestro ordenador, por si acaso ocurriese algún problema que nos impidiese acceder a los originales que tenemos en él. Esta copia también se denomina copia de respaldo o Backup en términos ingleses. Backup es sinónimo de protección de información.

Podemos perder nuestra información o cuando menos no poder acceder a ella por motivos muy diversos, lo cual, más aún, tratándose de un correo institucional tiene efectos en el normal desarrollo de las funciones de la entidad estatal que se desarrollan a través de sus servidores públicos o de sus contratistas. Al realizar dichas copias, deberá analizarse la importancia de la información, la periodicidad con que es necesario hacerlas y en qué lugar se resguardará la información (unidad interna o externa).

En el SENA, la multicitada Resolución No. 2159 estableció lo siguiente:

[…] 3. ACTIVOS DE INFORMACIÓN.

a) Es responsabilidad de los Directores de Área, Jefes de Oficina, Directores Regionales y Subdirectores de Centro de Formación Profesional Integral, asignar un responsable para cada activo de información que se encuentre prestando un servicio de TIC, en las instalaciones bajo su cargo.

b) El almacenamiento y las copias de respaldo de la información de la Entidad, deberá manejarse de acuerdo con el procedimiento que establezca la Oficina de Sistemas de la Dirección General.

[…]

d) Respecto a la privacidad y derechos de terceros: no está permitido acceder o copiar correo electrónico, direcciones, datos, programas u otros archivos sin permiso del titular.

[…]

f) Tanto los equipos y los programas instalados en ellos, así como los datos creados, almacenados y recibidos, son propiedad del SENA. Su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la Institución, serán sancionadas de acuerdo con las normas vigentes.

[…]

i) Todos los funcionarios y contratistas del SENA deberán velar por el cumplimiento y respeto a derechos de autor y copyright cuando se realice uso e instalación y adquisición de cualquier conjunto de programas informáticos, clasifíquense estos como software con propietario, semilibre, freeware previamente avalado y autorizado desde la Oficina de Sistemas. Y se prohíbe la instalación de programas informáticos que se clasifique en su uso como software Shareware, Warez, Trial, demos, abandonware. Al que se restringe la implementación y uso de software recibido en calidad de regalo, bono, plus, prebenda para la Entidad sin el debido acto administrativo de legalización de la donación.

f) Tanto los equipos y los programas instalados en ellos, así como los datos creados, almacenados y recibidos, son propiedad del SENA. Su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la Institución, serán sancionadas de acuerdo con las normas vigentes. (Subraya y negrilla fuera de texto)

Igualmente, establece la resolución en comento en cuanto a responsabilidades:

[…] 5.2 RESPONSABILIDADES FRENTE AL CORREO ELECTRÓNICO INSTITUCIONAL.

Es responsabilidad de todos los usuarios del correo institucional:

[…]

d) Realizar mensualmente copias de respaldo de sus archivos y de sus carpetas de mensajes de correo en el computador asignado para el cumplimiento de labores en la Entidad. Se entenderá que el contenido del buzón de correo está integrado por archivos en tránsito y no almacenados en forma permanente. Cada usuario es responsable de la actualización de dichas copias. Se debe enviar un manual para usuario el cual indique el proceso.

El mismo contenido se encuentra en la Resolución No. 284 de 2008, artículo 6[3], en cuanto al tema de responsabilidad.

Finalmente, es preciso advertir la existencia de la Mesa de Ayuda SENA, esta que se define como un equipo de trabajo, un punto de contacto entre la comunidad SENA y el Centro de Cómputo (Mesa de Ayuda), cuyo objetivo principal es responder de una manera oportuna, eficiente y con alta calidad a las peticiones relacionadas con los distintos aspectos de la tecnología de la información y la comunicación; es decir, que la Mesa de Ayuda da soporte en los distintos ámbitos que posee el SENA.

vi. DERECHOS DE AUTOR

Como lo describe el artículo 61 de la Constitución Política el Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley. Las disposiciones contenidas en la Decisión Andina 351 de 1993, las Leyes 23 de 1982 y 44 de 1993 y los Decretos 1360 de 1989 y 460 de 1995, establecen el régimen jurídico que regula la protección del derecho de autor y los derechos conexos. Así mismo se cuenta con la Directiva Presidencial 01 de 1999, la Directiva Presidencial 02 de 2002, y las Circulares de la Dirección Nacional de Derechos de Autor Nos. 04 de 2006, 12 de 2007 y 17 de 2011.

Así para la protección de los derechos de autor del titular de luna cuenta, deberá determinarse el contenido del mensaje del correo, pues si transmite una obra literaria, artística o científica, no habría duda; pero si se trata de un simple mensaje informativo no amerita tal protección. Se ha señalado por la doctrina internacional, que la protección de la propiedad intelectual del contenido de los mensajes de correo electrónico es limitada y por lo tanto relativa, en particular cuando se trata de breves mensajes de texto que permiten una conversación simultánea pero escrita, que pocas veces se constituye en una obra de protección de los derechos de autor.

Se ha señalado que el derecho de autor es un conjunto de normas que protegen los derechos subjetivos del creador de la obra, entendida esta como la manifestación personal, original de la inteligencia expresada de forma tal que pueda ser perceptible; la protección se concede desde el momento de la creación sin que se exija formalidad jurídica alguna. De dicha autoría se

desprenden derechos morales y derechos patrimoniales. Los derechos morales facultan al autor para reivnicidar en todo tiempo la paternidad de la obra, oponerse a toda deformación que demerite su creación, publicarla o conservarla inédita, moficarla y a retirarla de circulación. Estos derechos se caracterízan por ser instrsferibles, irrenuncaibles e inprescriptibles. Los derechos patrimoniales son el conjunto de prerrogativas del autor que le permiten explotar económicamente la obra, son una facultad exclusiva de autorizar su utilización, reproducción, comunicación y distribución, traducción o transformación de la obra. Estos derechos son susceptibles de transmitirse.[4]

De acuerdo con la Organización Mundial de la Propiedad Intelectual- OMPI, el objeto de protección del derecho de autor es “toda creación intelectual, original, expresada en un forma reproducible”. La Decisión Andina 351 de 1993, artículo 3, señaló como objeto de protección de dicho derecho “Toda creación intelectual originaria, de naturaleza artística, científico literaria susceptible de ser divulgada o reproducida de cualquier forma”.

Entonces son requisitos para proteger una obra:

a. Que sea una creación intelectual, producto del ingenio y la capacidad humana

b. Que sea original, es decir, cuente con un sello personal del autor que hace la obra única.

c. Que sea literario o artístico, esto se refiere a la forma de expresión de la obra

d. Que sea susceptible de ser divulgada o reproducia por cualquier medio

Existen dos tipos de titulares en el derecho de autor, el autor o titular originario, la persona natural que realizó la labor intelectual e creación artística o literaria, y el autor derivado, definido como quien ha recibido la titularidad de algunos de los derechos de autor, estos son terceros diferentes al creados que han adquirido derechos patrimoniales de aquél.

Ahora bien, si nos referimos a los derechos de autor sobre obras creadas por funcionarios o servidores públicos en ejercicio de sus funciones; tenemos que partiendo de que la titularidad de los derechos patrimoniales se puede adquirir por acto entre vivos, por causa de muerte o por disposición legal; en este caso las obras creadas por servidores públicos en cumplimiento de sus obligaciones se entiende por disposición legal cedidos desde el nacimiento de la obra todos los derechos patrimoniales que pueda tener el empleado público, sin embargo, conserva los derechos morales. Igualmente, las obras realizadas al margen de sus obligaciones conservan todas las prerrogativas patrimoniales de dichas creaciones intelectuales.

Finalmente, en el caso de los contratistas, deberá hacerse una remisión al contrato celebrado, y partiendo de que la obra sea de aquéllas que enmarca en la protección de derecho de autor, se analizará el tema de los derechos patrimoniales, por cuanto los derechos morales siempre recaerán en cabeza del titular originario.

En este orden de ideas, si se hace uso de contratistas para desarrollar la propiedad intelectual de una entidad, como por ejemplo el contratista que elabora programas informáticos, es necesario celebrar un contrato antes de iniciar el trabajo, con el fin de especificar quién es el titular de la propiedad intelectual y como se tratará a futuro. Así durante el trabajo pueden surgir derechos del contratista de ser el titular o el cotitular de la obra. Es mediante contratos que los derechos de propiedad intelectual pueden venderse, ser objeto de licencias o hasta cederse; de ello depende evitar un litigio a futuro.

Tenemos entonces que una cláusula de propiedad intelectual, entre otros, debe especificar la propiedad intelectual que se desarrollará en ejecución del contrato, variando si se trata de patentes y marcas, invenciones, propiedad industrial, etc. En caso de derechos de autor como el software o las bases de datos, es necesario regirse a cada derecho patrimonial y tener en cuenta la transferencia de derecho de explotación y las formas de utilización de las obras. Igualmente debe indicar que los derechos se ceden de manera exclusiva. Si no existe mención a la propiedad intelectual la empresa puede acogerse a las presunciones legales de cesión de derechos en su favor.

En el caso de software, bases de datos y otras obras originales protegidas por derechos de autor opera una presunción de cesión de derechos en favor del empleador o contratante (Artículo 28, Ley 1450 de 2011). Las invenciones desarrolladas por empleados le pertenecen al empleador en los casos en que este fue contratado para actividades de investigación o el desarrollo es resultado de las labores encargadas (Artículo 539 del Código de Comercio).

d. CONCLUSIONES

- Existen en el SENA políticas o reglamentos, en general normatividad, para el uso de los servicios de tecnologías de información y telecomunicaciones y recursos informáticos, tanto para contratistas como para funcionarios, en los términos expuestos.

- 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 contractual. Por tratarse de un servicio financiado con recursos públicos, el correo electrónico institucional no podrá ser utilizado por terceros. Igualmente los computadores, que se entienden como una herramienta para el cumplimiento de las funciones asignadas al cargo que desempeña el servidor público y del objeto contractual del contratista.

- La información transmitida por medio del correo electrónico institucional es considerada información oficial y debe ser manejada confidencialmente entre el remitente y los destinatarios. La cuenta de correo electrónico institucional asignada por el SENA, debe ser utilizada para atender los asuntos oficiales de la entidad.

- Es un deber de los servidores públicos utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función en forma exclusiva, el incumplimiento de tal conducta deriva en una responsabilidad disciplinaria. Igualmente, los contratistas responden por el buen o mal uso de los recursos y servicios relacionados con las TIC que tienen a su disposición con ocasión del objeto contractual.

- Respecto a la privacidad y derechos de terceros, no está permitido acceder o copiar correo electrónico, direcciones, datos, programas u otros archivos sin permiso del titular. Lo anterior salvo orden de autoridad competente.

- Se establece por acto administrativo que se deberán realizar mensualmente copias de respaldo de los archivos y de las carpetas de mensajes de correo en el computador asignado para el cumplimiento de labores en la Entidad, por cada titular de la cuenta.

- Tanto los equipos y los programas instalados en ellos, así como los datos creados, almacenados y recibidos, son propiedad del SENA. Su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la Institución, serán sancionadas de acuerdo con las

normas vigentes.

- Siempre que un empleado público realice una obra en cumplimiento de las funciones asignadas a su cargo, las cuales están contempladas en la constitucion, la ley o el manual de funcines de la entidad correspondiente, existe una presunción de transferencia en virtud de la cual los derechos patrimoniales serán de la entidad pública para la cual labora, salvo excepciones que consagre el legislador. Lo anterior no sin advertir que la obra debe ser de aquellas protegidas por el derecho de autor. Si se trata de un contratista habrá que remitirse a lo acordado en el contrato, siendo posible que sea el titular o cotitular de una obra protegida; si hay vacío habrá de acogerse a las presunciones y demás aspectos de ley.

- La Oficina de Sistemas de la Dirección General es la encargada de administrar, monitorear y hacer seguimiento del uso que el personal vinculado a la Entidad le dé al sistema de correo electrónico institucional.

- Los actos administrativos, acuerdos y resoluciones, expedidas por el SENA y la Oficina de Sistemas son de público conocimiento, es decir, son de conocimiento de los servidores públicos y contratistas del SENA.

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>.

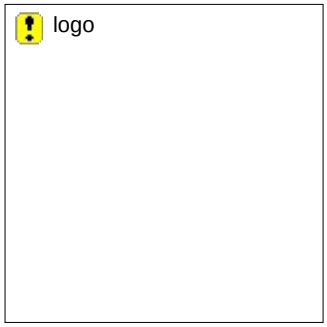
1. El uso legítimo del correo electrónico. https://delitosinformaticos.com/delitos/cor reo.shtml

2. Ministerio de las Telecomunicaciones. Términos y Condiciones de uso del correo electrónico. Bogotá D.C.

3. Artículo 6. […]4. Realizar copias mensualmente de respaldo de sus archivos y de sus carpetas de mensajes de correo en el computador asignado para el cumplimiento de labores en la Entidad. En consecuencia se entenderá que el contenido del buzón de correo está integrado por archivos en tránsito y no almacenados en forma permanente. Cada usuario es responsable de la actualización de dichas copias.

4. Dirección Nacional de Derechos de Autor. Rad. 1- 2007- 13593 del 15/05/2007

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