



ACUERDO No.

DE 201

Por medio del cual se aprueba la Política de Seguridad y Privacidad de la información y política de tratamiento para la protección de Datos personales, en el Servicio Nacional de Aprendizaje SENA, y se dictan otras disposiciones

EL CONSEJO DIRECTIVO NACIONAL O REGIONAL

En uso de las facultades legales, en especial por el numeral 1 y 22 del artículo 3o del Decreto 249 de 2004, y

CONSIDERANDO:

Que el artículo 15 de la Constitución Política consagra que *“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. Solo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley (...)”*

Que 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”*, 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 bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.

Que la ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales, la cual busca proteger la información de las personas que esté en poder de empresas públicas o entidades privadas, las cuales tienen la responsabilidad de adaptar sus procesos con el fin de realizar un manejo adecuado de sus bases de datos.

Que el Decreto 1377 de 2013, *“por el cual se reglamenta parcialmente la Ley 1581 de 2012”*, establece en su artículo 13 que los responsables del tratamiento de la información deberán desarrollar sus políticas para el tratamiento de los datos personales y velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas.

Que 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 cuyo objeto es 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, y constituye el marco general de la protección del ejercicio del derecho de acceso a la información pública en Colombia.

Que el Decreto 103 de 2015, por el cual se reglamenta parcialmente la Ley 1712 de 2014, en los temas relacionados con la gestión de la información pública en cuanto a su publicación, divulgación, recepción y respuesta a solicitudes de acceso a esta, su adecuada clasificación y reserva, elaboración de los instrumentos de gestión de información, así como el seguimiento de la misma.

Que el Conpes 3854 de 2016, establece la Política Nacional de Seguridad Digital en la República de Colombia.



ACUERDO No.

DE 201

Por medio del cual se aprueba la Política de Seguridad y Privacidad de la información y política de tratamiento para la protección de Datos personales, en el Servicio Nacional de Aprendizaje SENA, y se dictan otras disposiciones

Que el Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3. Principios. Define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera en el artículo 2.2.9.1.2.1., define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales, los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

Que en el marco de las funciones previstas en el artículo 10 del Decreto 249 de 2004, le compete a la Dirección de Planeación y Dirección de Planeación Corporativo del SENA:” 17. Definir y liderar el almacenamiento, custodia, seguridad y disponibilidad de la información en medios electrónicos en el SENA.

Que mediante el Acuerdo No. 009 de 2016, se aprobó la Política de tratamiento para la protección de Datos Personales en el Servicio Nacional de Aprendizaje SENA, y se adoptó el instructivo de Política de Protección de Datos Personales.

Que El SENA, como entidad pública adscrita al Ministerio de Trabajo, dispone de un marco legal aplicable conforme a las leyes vigentes y un marco normativo de referencia basado en estándares y buenas prácticas de seguridad, con el objetivo de proteger y preservar los activos de información, desarrollar e implementar el modelo de seguridad y privacidad de la información y el SGSI de la entidad, así como garantizar los objetivos y funciones del SENA; dando cumplimiento a la normatividad vigente so pena de incurrir en las sanciones previstas en la ley.

De allí la importancia de establecer políticas claras para la Entidad, que permitan proteger la Información y los datos personales, señalados en un solo acto administrativo, lo que permitirá establecer lineamientos actualizados estandarizando procesos y estableciendo ejercicios de aseguramiento de la Información, teniendo en cuenta los requisitos legales, operativos, tecnológicos, de seguridad con el fin de asegurar el cumplimiento de la integridad, disponibilidad, legalidad y confidencialidad de la información.

En mérito de lo expuesto,

ACUERDA

Artículo 1º. Aprobar y adoptar las Política de Seguridad y Privacidad de la Información y la Política de Protección de Datos Personales en el Servicio Nacional de Aprendizaje (SENA), en los siguientes términos:

CAPITULO I

DISPOSICIONES GENERALES

Artículo 2º. Propósito: Las presentes Políticas describen el compromiso de la Alta Dirección y la necesidad del Servicio Nacional de Aprendizaje – SENA, de definir las bases de gobernanza para gestionar y preservar de manera efectiva la confidencialidad, integridad, disponibilidad y privacidad de sus activos de información; tiene como finalidad apoyar el cumplimiento de los objetivos definidos dentro del Plan Estratégico Institucional, promoviendo buenas prácticas y aplicando controles que permitan el uso adecuado de la información en el logro de la misión, visión y objetivos transformacionales de la Entidad.

Artículo 3º. Alcance: Las Políticas de Seguridad y Privacidad de la Información y Política de Protección de Datos Personales, aplican a todos los servidores públicos, trabajadores oficiales, contratistas, instructores, aprendices, practicantes, proveedores y demás grupos de



Por medio del cual se aprueba la Política de Seguridad y Privacidad de la información y política de tratamiento para la protección de Datos personales, en el Servicio Nacional de Aprendizaje SENA, y se dictan otras disposiciones

interés que accedan a la información del Servicio Nacional de Aprendizaje – SENA; la cual es de obligatorio cumplimiento.

Artículo 4°. Declaración de la Política General de Seguridad y Privacidad de la información y Política de Protección de Datos Personales: Mediante estas políticas, el Servicio Nacional de Aprendizaje – SENA reconoce la información como un activo fundamental que se debe proteger adecuadamente para el desarrollo de las actividades de la Entidad, en donde la privacidad y la seguridad de esta información y el conocimiento generado tienen una importancia primordial en el cumplimiento de su Plan Estratégico Institucional vigente.

La Dirección de Planeación y Direccionamiento Corporativo, Definirá y liderará la gestión, adopción, implementación, operación, seguimiento, mantenimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información – MSPI - del SENA, asignando y comunicando las funciones, responsabilidades y recursos necesarios para que las políticas de Seguridad y Privacidad de la Información y de Protección de Datos Personales se integre a todos los procesos de la Entidad.

Artículo 5°. Objetivo General: Determinar los lineamientos que permitan proteger la Información y los datos personales que adopta el Servicio Nacional de Aprendizaje SENA, a través de acciones de aseguramiento de la Información teniendo en cuenta los requisitos legales, operativos, tecnológicos, de seguridad y de la entidad alineados con el contexto de direccionamiento estratégico y de gestión del riesgo con el fin de asegurar el cumplimiento de la integridad, disponibilidad, legalidad y confidencialidad de la información.

La Seguridad de la Información es una prioridad para El servicio Nacional de Aprendizaje SENA, por lo tanto, es responsabilidad de todos los funcionarios y contratistas de la Entidad velar por el continuo cumplimiento de las políticas definidas.

Artículo 6°. Objetivos Específicos: Esta política establece una serie de objetivos que regulan las actividades relacionadas con la Seguridad y la Privacidad de la Información en la Entidad, como son:

- a. Establecer lineamientos y políticas de seguridad y privacidad de la información que definan las directrices formales de actuación en la Entidad.
- b. Definir, gestionar y mantener roles y responsabilidades en materia de Seguridad y Privacidad de la Información que apoyen la gestión del Modelo definido en la entidad.
- c. Mantener actualizadas las políticas y procedimientos relacionados con la Seguridad y Privacidad de la Información.
- d. Proteger la información del SENA durante todo su ciclo de vida, mediante la implementación de buenas prácticas y controles efectivos que busquen preservar la confidencialidad, integridad y disponibilidad.
- e. Garantizar el cumplimiento de las obligaciones legales, regulatorias o contractuales de la Entidad que se encuentren relacionadas con la Seguridad y Privacidad de la Información.
- f. Dar una respuesta oportuna y adecuada en caso de materializarse un evento que pudiera afectar la disponibilidad de los recursos que son indispensables para el desarrollo de las diferentes actividades de la Entidad, personas, locaciones, tecnología, información o proveedores.



Por medio del cual se aprueba la Política de Seguridad y Privacidad de la información y política de tratamiento para la protección de Datos personales, en el Servicio Nacional de Aprendizaje SENA, y se dictan otras disposiciones

- g. Garantizar la seguridad de la información con el fin de mantener su integridad y la continuidad del acceso a la información ante situaciones adversas que se pudieran presentar en la Entidad,
- h. Identificar, analizar, evaluar y tratar los riesgos de seguridad de la información para mitigar los conflictos catalogados como altos y extremos, con el fin de prevenir o reducir su impacto sobre el normal desarrollo de las actividades de la Entidad.
- i. Garantizar una adecuada gestión de incidentes, eventos o debilidades de seguridad de la información, reduciendo su impacto, propagación y duración.
- j. Fortalecer el conocimiento y las habilidades en seguridad y privacidad de la información en la comunidad SENA.
- k. Sensibilizar al personal de la entidad en el uso adecuado, la importancia y protección de los activos de información.
- l. Definir, implementar, operar y mejorar continuamente el Modelo de Seguridad y Privacidad de la Información – MPSI- del SENA aumentando y manteniendo el nivel de madurez requerido por la entidad.

Artículo 7º. Términos y Definiciones:

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.
- **Aviso de privacidad:** Comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.
- **Base de datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento.
- **Datos abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.
- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Dato público.** Es aquel dato que no es semiprivado ni privado ni sensible son considerados datos públicos entre otro lo relativo al estado civil de las personas a su profesión u oficio y a su calidad de comerciante o servidor público. Por su naturaleza los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas o boletines oficiales y sentencia judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- **Dato privado:** Es el dato que por su naturaleza íntima o reservada solo es relevante para el titular.



Por medio del cual se aprueba la Política de Seguridad y Privacidad de la información y política de tratamiento para la protección de Datos personales, en el Servicio Nacional de Aprendizaje SENA, y se dictan otras disposiciones

- **Dato semiprivado:** Es aquel dato que no tiene una naturaleza íntima, reservada ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular, sino a un grupo de personas o a la sociedad en general. Para su tratamiento se requiere de la autorización de su titular.
- **Dato sensible:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos
- **Documento de Archivo:** Es el registro de información producida o recibida por una entidad pública o privada en razón de sus actividades o funciones.
- **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.
- **Información:** Se refiere a un conjunto organizado de datos contenido en cualquier documento que los responsables y/o encargados del tratamiento generen obtengan, adquieran, transformen o controlen.
- **Información pública:** Es toda información que el responsable y/o encargado del tratamiento, genere, obtenga, adquiera, o controle en su calidad de tal.
- **Información Pública Clasificada:** Es aquella información que estando en poder de un sujeto responsable en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica, por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en la ley.
- **Información Pública Reservada:** Es aquella información que estando en poder de un sujeto responsable en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos.
- **Responsable del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre los datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- **Transferencia:** La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.
- **Transmisión:** Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable.

CAPÍTULO II



Por medio del cual se aprueba la Política de Seguridad y Privacidad de la información y política de tratamiento para la protección de Datos personales, en el Servicio Nacional de Aprendizaje SENA, y se dictan otras disposiciones

POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION

Artículo 8°. Adoptar el Manual de Política de Seguridad de la Informacion en el Servicio Nacional de Aprendizaje, SENA, cuyo documento anexo al presente Acuerdo forma parte integral del mismo.

Parágrafo: Del Manual de la Política de Seguridad de la Informacion SENA se señalaran los lineamientos específicos, técnicos u operativos que apoyan la gestión de la Seguridad y Privacidad de la Información en la Entidad; permitiendo la integración del sistema integrado de gestión y autocontrol – SIGA con el subsistema de seguridad de la información; llevando la implementación de los controles necesarios para salvaguardar la información del SENA desde la dirección general hasta sus centros de formación.

CAPÍTULO III

POLITICA GENERAL DE PROTECCION DE DATOS

Artículo 9°. Adoptar el Manual de Política de Protección de Datos Personales en el Servicio Nacional de Aprendizaje, SENA, cuyo documento anexo al presente Acuerdo forma parte integral del mismo.

CAPÍTULO IV OTRAS DISPOSICIONES

Artículo 10 ° Responsabilidades: Será responsabilidad del Comité Institucional de Gestión y Desempeño del Servicio Nacional de Aprendizaje SENA, o quien haga sus veces, asegurar la implementación y desarrollo del Modelo de Seguridad y Privacidad de la Información, así como la política de Protección de Datos Personales.

Parágrafo: Sera la Direccion de Planeacion y Direccionamiento Corporativo quien presente ante el Consejo Directivo Nacional, para su aprobación y/o modificación la política y objetivos del Modelo de Seguridad y Privacidad de la Información, así como como la política de Protección de Datos Personales.

Artículo 11 ° Responsable de la Seguridad de la Informacion: Será responsabilidad de la Direccion de Planeacion y Direccionamiento Corporativo, planificar, desarrollar, y gestionar las políticas y lineamientos del Modelo de Seguridad y Privacidad de la Información para la Entidad.

Artículo 12° Responsable del Tratamiento de Datos Personales: El Servicio Nacional de Aprendizaje – SENA, actuará como responsable del tratamiento de Protección de datos personales y hará uso de los mismos únicamente para las finalidades que se encuentra facultado, especialmente las señaladas en la ley reglamentaria y la normatividad vigente.

Artículo 13°. Encargado del tratamiento de Datos Personales: Será el Director de la Entidad a través de resolución, quien designe esta actividad a funcionario competente en esta materia, quien además deberá respetar las condiciones de seguridad y privacidad de la información de los titulares de la información.

Artículo 14°. Revisión: La Política de seguridad y privacidad de la información y la de Protección de Datos Personales será revisada anualmente, o antes en el caso que amerite su modificación; este proceso será liderado por la Direccion de Planeacion y



ACUERDO No.

DE 201

Por medio del cual se aprueba la Política de Seguridad y Privacidad de la información y política de tratamiento para la protección de Datos personales, en el Servicio Nacional de Aprendizaje SENA, y se dictan otras disposiciones

Direccionamiento Corporativo, y será revisado y aprobado por el Comité Institucional de Gestión y Desempeño del Servicio Nacional de Aprendizaje SENA.

Artículo 15°. Comuníquese el presente Acuerdo a la Secretaría General, Directores de área, Jefes de Oficina de la Dirección General, Directores Regionales y Subdirectores de Centros de Formación Profesional del SENA para su conocimiento y aplicación.

Artículo 16°: El presente Acuerdo rige a partir de la fecha de su publicación en el Diario Oficial; y Deroga el acuerdo 009 de 2016 y demás que le sean contrarias; de conformidad con el artículo 8 de la Ley 1437 de 2011 publíquese en la página web del SENA.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE (Según se requiera)

Dado en (Ciudad de origen y fecha)

Nombre y Apellido
Presidente

Nombre y Apellido
Secretario

Vo.Bo. Juan Fernando Lopez Mejia, Director de Planeación y Direccionamiento Corporativo

Vo.Bo. Óscar Julián Castaño Barreto - Director Jurídico

Revisó: Antonio José Trujillo Illera, Coordinador Grupo de Conceptos Jurídicos y Producción Normativa

Revisó: Gloria Acosta Contreras, Profesional Dirección Jurídica

Proyectó: Julio Cesar Mancipe Oficial de Seguridad de la Informacion -SENA

Proyectó: Mayerly Garzon Rico- Asesora Jurídica -Dirección de Planeación y Direccionamiento Corporativo



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION

SENA

Tabla de contenido

Introducción	2
1. Gestión sobre las Políticas de Seguridad de la Información	3
2. Organización de Seguridad de la Información	4
2.1 Roles y Responsabilidades	4
2.2 Dispositivos Móviles y Teletrabajo	5
3. Seguridad de los Recursos Humanos	5
3.1 Antes de Asumir el Empleo	5
3.2 Durante la Ejecución del Empleo	6
3.3 Terminación y Cambio de Empleo	7
4. Gestión de Activos	8
4.1 Responsabilidad por los Activos de Información	8
4.1.1 Responsabilidad por los Activos de Información	8
4.2 Clasificación de la Información	9
4.2.1 Clasificación y Manejo de la Información	10
4.2.2 Etiquetado de la información	10
4.3 Manejo de los soportes de almacenamiento	10
4.4.1 Gestión de soporte extraíbles	10
5 Control de Acceso	11
6 Seguridad Física y Ambiental	11
7 Cifrado	11
8 Seguridad de las Operaciones	11
9 Seguridad de las Comunicaciones	11
10 Adquisición, Desarrollo y Mantenimiento de Sistemas	11



11 Relaciones con los Proveedores.....	11
12 Gestión de Incidentes de Seguridad de la Información	12
13 Cumplimiento	12

Introducción

El Servicio Nacional de Aprendizaje – SENA, viene desplegando e implementando su política de seguridad y privacidad de la Información a nivel nacional y para dar cumplimiento a los objetivos de seguridad que se han definido a través de dicha política.

El manual de políticas de seguridad de la información consiste en una serie de lineamientos, directrices que le permiten al SENA establecer criterios para asegurar su información, protegerla, procesarla, compartirla, administrarla; llegando a la aplicación de controles de seguridad que reduzcan los riesgos y las vulnerabilidades. El manual de políticas de seguridad tiene como propósito, la integridad, confidencialidad y disponibilidad de la información de SENA.

El SENA a través de la Dirección de Planeación y de la Oficina de Sistemas, divulga y socializa las políticas y controles que se deriven de esta; con el fin de que los usuarios del SENA y partes interesadas adopten una postura de seguridad, para proteger la información y evitar su divulgación no autorizada.

Este manual formaliza el compromiso de la Alta Dirección frente a la gestión de la seguridad de la información y presenta de manera escrita a los usuarios el compendio de acciones con las cuales el SENA establece las normas para proteger de posibles riesgos de daño, pérdida y uso indebido de la información, los equipos y demás recursos informáticos de la Entidad, los cuales están en constante cambio y evolución de acuerdo con el avance de la tecnología y los requerimientos de la Entidad.

Con el presente documento se define el conjunto de políticas que conforman el manual de políticas del SENA.

El presente manual resguarda los siguientes dominios de seguridad.

1	Gestión sobre las políticas de seguridad de la Información
----------	---



2	Organización de seguridad de la Información
3	Seguridad de los Recursos Humanos
4	Gestión de Activos
5	Control de Acceso
6	Seguridad Física y Ambiental
7	Cifrado
8	Seguridad de las operaciones
9	Seguridad de las comunicaciones
10	Adquisición, desarrollo y mantenimiento de sistemas
11	Relaciones con los proveedores
12	Gestión de incidentes de seguridad de la información
13	Cumplimiento

1. Gestión sobre las Políticas de Seguridad de la Información

El SENA a través de la Dirección de Planeación emitirá lineamientos para la gestión de la seguridad de la información al interior de la entidad, de manera que dicha administración de seguridad, su implementación, funciones y responsabilidades, permitan aplicar las medidas de seguridad necesarias para la protección de la información de la entidad.

El manual de políticas de seguridad de la información será el elaborado por el CISO, en compañía de la Dirección de Planeación, de la dirección Jurídica y de la Oficina de Sistemas, para ser aprobado por el comité directivo.

La Dirección de Planeación y la oficina de sistemas, realizarán las gestiones necesarias para que el manual de políticas de seguridad de la información o políticas complementarias sean comunicadas a todo nivel en el SENA.



El CISO y las áreas competentes deberán revisar y actualizar las políticas de seguridad de la información contenidas en el presente documento una vez al año o cuando los cambios en el entorno así lo exijan.

El subsistema de Seguridad de la información de la entidad deberá ser gestionado por la oficina de Sistemas, en el cual se contemplen los diferentes dominios de Seguridad expuestos en el presente manual.

2. Organización de Seguridad de la Información

El SENA a través del gobierno de la seguridad, establece y define unos roles y responsabilidades que permitan desarrollar actividades propias de seguridad como son la operación, gestión y administración.

El CISO o quien haga sus veces debe identificar las autoridades a cuáles acudir en caso de un incidente de seguridad y mantener contactos con grupos de interés del ámbito de seguridad que le permitan mejorar su gestión.

La oficina de sistemas debe velar por el mantenimiento del SGSI, con el fin de garantizar la ejecución de controles y seguimiento a los mismo.

Las iniciativas o proyectos desarrollados por el SENA deben estar alineados con las políticas y manual de seguridad de la información.

2.1 Roles y Responsabilidades

Propietario:

El Sena es propietario de los activos de información; los propietarios son los responsables de clasificar la información, establecer el nivel de criticidad y disponibilidad de esta.

Responsable:

Son los directores, coordinadores, supervisores, jefes de oficina, directores regionales, subdirectores regionales; tendrán como responsabilidad asegurar la información de su área, controlando que se cumplan los requerimientos de seguridad de acuerdo con lo indicado por los propietarios de la información y las medidas implementadas por el Custodio.

Custodio:



La oficina de sistemas es la responsable de implementar las medidas y controles necesarios para salvaguardar los activos de información de acuerdo con la clasificación establecida por los propietarios.

Usuario:

Los servidores públicos, aprendices, contratistas y toda aquella persona que se conecte a la red del SENA o utilicen los activos de información, tienen la responsabilidad hacer buen uso del acceso a la información suministrada para el cumplimiento de sus funciones.

2.2 Dispositivos Móviles y Teletrabajo

Los equipos o dispositivos móviles que hagan uso de la información del SENA o que se conecten a sus redes se deben acoger a las políticas de seguridad de la información definidas en el presente manual.

Al conectar un equipo o un dispositivo a la red del SENA, el propietario de dicho equipo o dispositivo acepta las políticas definidas en el presente manual y así mismo, las disposiciones que estas determinen.

La Oficina de Sistemas debe disponer de un mecanismo de conexión segura que garantice que las conexiones de teletrabajo autorizadas por el SENA se realicen de forma segura y se protegen los activos de información en uso.

3. Seguridad de los Recursos Humanos

3.1 Antes de Asumir el Empleo

La Secretaria General, quien coordina el grupo de Relaciones laborales, es la encargada de realizar las siguientes actividades relacionadas con el proceso de selección e ingreso de personal al SENA, las cuales son actividades fundamentales para la seguridad de la información.

- Verificar los antecedentes de todos los aspirantes a un empleo, de acuerdo con:
 - Las leyes, reglamentos y ética vigentes en el SENA y el país.
 - La clasificación de la información a la cual se va a tener acceso.
 - Los riesgos percibidos.
- Confirmar la información de referencias personales, familiares y comerciales, para los casos en los que el aspirante vaya a tener acceso a información considerada sensible.
- Realizar una verificación completa de la hoja de vida del aspirante.



- Solicitar una confirmación de las certificaciones académicas y profesionales entregadas en la hoja de vida, en caso de sospecha sobre su legitimidad.
- Realizar una verificación de identidad independiente (pasaporte o documento similar).
- Realizar todas las verificaciones necesarias para confirmar la veracidad de la información suministrada por el aspirante a ocupar un cargo antes de su vinculación definitiva.
- Certificar que los servidores públicos del SENA que en razón de su cargo deban tener acceso a información del SENA, firmen en calidad de aceptación un Acuerdo de Confidencialidad, en el cual se les informe de la existencia de las políticas contenidas en el presente manual, documento que deberá ser adjuntado a los demás documentos relacionados con la ocupación del cargo.

Las áreas encargadas de la contratación, jurídica, compras, de la dirección general, regionales y centro de formación del SENA, serán las encargadas de realizar las siguientes actividades fundamentales para la seguridad de la información, según corresponda en cada caso:
Certificar que el personal provisto por terceros (contratistas, temporales, etc.), que en razón de sus funciones deban tener acceso a información de la entidad firmen en calidad de aceptación un Acuerdo de Confidencialidad, antes de otorgar acceso a las instalaciones o a las plataformas tecnológicas.

3.2 Durante la Ejecución del Empleo

La alta dirección del SENA, en razón de proteger la información y los recursos tecnológicos de la entidad y como demostración del apoyo a la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), promoverán la cultura de seguridad de la información a todo nivel en la entidad, de manera que se define lo siguiente:

- El equipo directivo debe mostrar su compromiso con la seguridad de la información por medio de la aprobación y apoyo a la implantación del presente manual de políticas de seguridad de la información.
- El SENA debe promover la importancia de la seguridad de la información entre todos los funcionarios, contratistas, aprendices, así como motivar el entendimiento, la toma de conciencia y el cumplimiento de las políticas, normas, procedimientos y estándares establecidos.
- El equipo directivo debe definir y establecer los procesos disciplinarios y el tratamiento que se le dará a los casos de incumplimiento al presente manual de políticas de seguridad de la información.
- Para el caso de los aprendices estará basado en el régimen estudiantil, para los instructores por medio del código que le aplique (si es de planta, si es contratista) y reglamento de Trabajo, para los funcionarios o contratistas el reglamento de trabajo; se deben aplicar los respectivos procesos disciplinarios cuando se identifiquen violaciones o incidentes de seguridad que así lo ameriten.



- La dirección de Planeación en conjunto con la Oficina de Sistemas, serán los encargados de convocar a los directivos, funcionarios, contratistas, aprendices a las sensibilizaciones, charlas, talleres y eventos programados como parte del plan de comunicaciones en seguridad de la información que se realizará de manera anual y deben proveer los recursos para su ejecución y controlar la asistencia.
- La dirección de Planeación en conjunto con la Oficina de Sistemas, serán los encargados de convocar a la comunidad de aprendices, a las sensibilizaciones y eventos programados como parte del plan de comunicaciones en seguridad de la información que será anual y así mismo deben proveer los recursos para su ejecución y controlar la asistencia.
- La comunidad de aprendices que por su cargo hagan uso de información del SENA o custodiada por ésta, deben dar cumplimiento a lo indicado en el presente manual de políticas de seguridad de la información y asistir a las sensibilizaciones y eventos a los cuales sean convocados como parte del plan de comunicaciones de seguridad de la información.
- Todo el personal de SENA, (directivos, contratistas, aprendices) no deben divulgar información confidencial del SENA ni por escrito ni en forma verbal. De la misma manera, aplica para situaciones donde la revelación de información pueda causar un impacto operativo, reputacional o legal para el SENA.

3.3 Terminación y Cambio de Empleo

El SENA garantizará que sus funcionarios serán desvinculados o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura, por lo tanto, define lo siguiente:

- La Secretaría General a través del grupo de relaciones laborales debe realizar el procedimiento de desvinculación, permiso de licencias, incapacidades, vacaciones o cambio de labores de los funcionarios del SENA llevando a cabo los procedimientos que la Secretaría General haya establecido.
- Los directores, coordinadores y Jefes de Oficina, directores y subdirectores regionales deben reportar de manera inmediata al grupo de relaciones laborales de la secretaria general, la desvinculación o cambio de labores de los funcionarios, contratistas, aprendices o del personal provisto por terceras partes, con el fin que se tomen las medidas pertinentes y a su vez se informe a las áreas interesadas.



4. Gestión de Activos

4.1 Responsabilidad por los Activos de Información

La información, los sistemas, los servicios y los equipos (estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, Servidores, aplicaciones, teléfonos, entre otros) del SENA, son activos de la entidad y se proporcionan a los funcionarios, contratistas, aprendices y a terceros autorizados, para cumplir con los propósitos institucionales.

Todos los activos de información del SENA deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que se parametrizaron en la guía de clasificación de activos de la información.

4.1.1 Responsabilidad por los Activos de Información

- Los directores, coordinadores, Jefes de Oficina, directores y subdirectores regionales deben actuar como responsable de la información física y electrónica de las dependencias a cargo, ejerciendo así la facultad de aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin.
- Los directores, coordinadores, Jefes de Oficina, directores y subdirectores regionales como responsable de los activos de información deben generar un inventario de dichos activos para las áreas o procesos que lideran, acogiendo las indicaciones de la guía de clasificación de la información con el apoyo del Oficial de Seguridad de la Información o del funcionario encargado del tema de riesgos.
- Los directores, coordinadores, Jefes de Oficina, directores y subdirectores regionales como responsables de los activos de información deben monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información cada seis meses.
- La Oficina de Sistemas puede realizar monitoreo sobre los activos de información del SENA sin que esto identifique a usuarios particulares. Este procedimiento se podrá llevar a cabo siempre y cuando se tengan indicios de su vinculación a un incidente de seguridad, de igual manera esta labor debe realizarse bajo la autorización del involucrado.
- Los activos de información del SENA pueden y deben ser utilizados por toda la comunidad del SENA, de acuerdo con las políticas contenidas en el presente manual y según la normatividad vigente nacional. Esto con el fin de evitar un impacto operativo, legal o reputacional para la entidad.
- Los directores, coordinadores, Jefes de Oficina, directores y subdirectores regionales deben utilizar los recursos tecnológicos de la entidad, con el único objetivo de llevar a cabo las labores asignadas al cargo; por consiguiente, no deben ser utilizados para fines ajenos a este.
- Los aprendices deben utilizar los recursos tecnológicos del SENA, como son los laboratorios de cómputo, servicios web, entre otros, con el único fin de sacar provecho a



las herramientas para la formación en el ámbito educativo; por consiguiente, no deben ser utilizados para fines ajenos a este.

- Si los directores, coordinadores, Jefes de Oficina, directores y subdirectores regionales, contratistas, aprendices requieren utilizar equipos propios diferentes a los proporcionados por la institución, deben solicitar la autorización, verificación y registro de la Oficina de Sistemas.
- Todo el personal del SENA y terceros deben cumplir con los controles mínimos de seguridad establecidos (antivirus, sistema operativo con parches de seguridad), por la Oficina de Sistemas para poder conectarse a la red del SENA.
- Todo el personal del SENA y tercero, cuando requiera instalar, hacer uso o compartir software (libre o propio) en los recursos proporcionados por la entidad, deben solicitar la autorización, verificación y registro de la Oficina de Sistemas.
- Todo el personal del Sena en el momento de desvinculación o cambio de labores, deben realizar la entrega de su puesto de trabajo al director o Jefe de Oficina o a quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.
- La Oficina de Sistemas debe establecer un inventario con el software y sistemas de información que se encuentran permitidos en las estaciones de trabajo de la entidad para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado en dichas estaciones de trabajo o equipos móviles corresponda únicamente al permitido.

4.2 Clasificación de la Información

El SENA definirá los niveles más adecuados para clasificar su información, de acuerdo a la normatividad vigente y a la sensibilidad identificada; la oficina de sistemas generará una guía de clasificación de la Información para que los propietarios de esta la cataloguen y determinen los controles requeridos para su protección.

Toda la información debe ser identificada, clasificada y documentada de acuerdo con la guía de Clasificación de la Información establecida.

La Guía de Clasificación de la Información define los controles técnicos y administrativos que se aplicaran en la entidad con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos en función de su nivel de clasificación.



4.2.1 Clasificación y Manejo de la Información

Todo el personal de SENA debe cumplir con los lineamientos establecidos en el manual de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la institución.

La secretaria general a través del grupo de gestión documental debe tener un periodo de almacenamiento para la información física y digital, el cual puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado previamente por el propietario de la información y cuando se cumpla el periodo de expiración, toda la información debe ser eliminada adecuadamente.

4.2.2 Etiquetado de la información

La información almacenada en medios magnéticos se deberá inventariar, anexando la descripción y las especificaciones de la misma, clasificándola y etiquetándola en los mismos niveles establecidos en clasificación de la información.

4.3 Manejo de los soportes de almacenamiento

La entidad evitará la divulgación no autorizada, la modificación, eliminación o destrucción de la información almacenada en los medios de almacenamiento dispuestos para tal fin.

4.4.1 Gestión de soporte extraíbles

La Oficina de Sistemas como responsable de proporcionar los medios, mecanismos o herramientas tecnológicas realizará la gestión de medios extraíbles de acuerdo a las necesidades de cada usuario respecto a las labores desempeñadas.



5 Control de Acceso

La entidad garantizará entornos con controles de acceso idóneos, los cuales aseguren el perímetro, tanto en oficinas, aulas de clase, salas de cómputo y laboratorios, así como en entornos abiertos para evitar el acceso no autorizado a ellos.

6 Seguridad Física y Ambiental

La entidad proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones. Así mismo, controlará de amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

7 Cifrado

La Entidad, asegurará el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información confidencial de la entidad al momento de almacenarse o transmitirse.

8 Seguridad de las Operaciones

La Oficina de Sistemas debe realizar la documentación y actualización de los procedimientos relacionados con la operación y administración de los sistemas de información de la institución

9 Seguridad de las Comunicaciones

La entidad a través de la Oficina de Sistemas, los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios tecnológicos que soportan la operación de la misma; así mismo, velará para que se tengan los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se envía a través de dichas redes de datos.

10 Adquisición, Desarrollo y Mantenimiento de Sistemas

La entidad, asegurará que el software adquirido y desarrollado tanto al interior de la misma como por terceras partes, cumplirá con los requisitos de seguridad y calidad establecidos por él. Las áreas propietarias de sistemas de información y la Oficina de Sistemas incluirán requisitos de seguridad en la definición de requerimientos y posteriormente se asegurarán que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.

11 Relaciones con los Proveedores



La entidad, establecerá mecanismos de control en sus relaciones con los proveedores, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información.

12 Gestión de Incidentes de Seguridad de la Información

La Oficina de Sistemas presentará un reporte de incidentes relacionado con la seguridad de la información a la directiva institucional.

13 Cumplimiento

La entidad velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ellas la referente a derechos de autor y propiedad intelectual, razón por la cual estará pendiente que el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

14 Privacidad y Protección de información de datos personales

El SENA garantizar que los datos personales almacenados en los sistemas de información, repositorios y recursos informáticos de la entidad, reciban una protección óptima, para preservar la confidencialidad, integridad y disponibilidad de los mismos.

El lineamiento dedicado a la Privacidad y Protección de Datos Personales será aplicado por todas las áreas que procesan datos personales, adicional a la oficina de sistemas, direcciones, coordinaciones y todos los servidores públicos, terceros, contratistas, partes interesadas, aprendices y proveedores de la entidad.

Para el cumplimiento de la Privacidad y Protección de Datos Personales, la entidad debe identificar los sistemas de información, repositorios y recursos informáticos que almacenan, recolectan y procesan datos personales, para fines institucionales. Con base en las normas vigentes, caso la Ley 1581 de 2012 o Ley de Protección de Datos Personales.



SERVICIO NACIONAL DE APRENDIZAJE SENA

FORMATO DE MEMORIA JUSTIFICATIVA

1. Proyecto de Normatividad	Acuerdo del Consejo Directivo Nacional para la aprobación y adopción de la Política de Seguridad de privacidad de la información, y modificación del Acuerdo 009 de 2019 “la Política de tratamiento para la protección de Datos Personales”.
2. Dependencia o Grupo responsable	Dirección de Planeación y Dirección de Planeación Corporativa .
3. Fecha de elaboración	07 de octubre de 2019
4. Documentos base aportados	Ley 1266 de 2008. Ley Estatutaria 1581 de 2012. Decreto 1377 de 2013. Ley 1712 de 2014. Decreto 103 de 2015. Conpes 3854 de 2016. Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018. Acuerdo 009 de 2016.

I. ANTECEDENTES, OPORTUNIDAD Y CONVENIENCIA

1. ANTECEDENTES:

Que el artículo 15 de la Constitución Política consagra que “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.

Que la Ley 1266 de 2008, 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 bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.

Que la ley Estatutaria 1581 de 2012, busca proteger la información de las personas que estén en poder de empresas públicas o entidades privadas, las cuales tienen la responsabilidad de adaptar sus procesos con el fin de realizar un manejo adecuado de sus bases de datos.

Que el Decreto 1377 de 2013, establece en su artículo 13 que los responsables del tratamiento de la información deberán desarrollar sus políticas para el tratamiento de los datos personales y velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas.

Que la Ley 1712 de 2014, 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, y constituye el marco general de la protección del ejercicio del derecho de acceso a la información pública en Colombia.



SERVICIO NACIONAL DE APRENDIZAJE SENA FORMATO DE MEMORIA JUSTIFICATIVA

Que el Decreto 103 de 2015, reglamenta parcialmente la Ley 1712 de 2014, en los temas relacionados con la gestión de la información pública en cuanto a su publicación, divulgación, recepción y respuesta a solicitudes de acceso a esta, su adecuada clasificación y reserva, elaboración de los instrumentos de gestión de información, así como el seguimiento de la misma.

Que a través del Conpes 3854 de 2016 se establece la Política Nacional de Seguridad Digital en la República de Colombia.

Que el Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3. Principios. Define la *seguridad de la información como principio de la Política de Gobierno Digital*, de igual manera en el artículo 2.2.9.1.2.1., define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales, los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

Que mediante el Acuerdo No. 009 de 2016, se aprobó la Política de tratamiento para la protección de Datos Personales en el Servicio Nacional de Aprendizaje SENA, y se adoptó el instructivo de Política de Protección de Datos Personales.

2. RAZONES DE OPORTUNIDAD Y CONVENIENCIA:

Que El SENA, como entidad pública adscrita al Ministerio de Trabajo, dispone de un marco legal aplicable conforme a las leyes vigentes y un marco normativo de referencia basado en estándares y buenas prácticas de seguridad, con el objetivo de proteger y preservar los activos de información, desarrollar e implementar el modelo de seguridad y privacidad de la información y el SGSI de la entidad, así como garantizar los objetivos y funciones del SENA; dando cumplimiento a la normatividad vigente so pena de incurrir en las sanciones previstas en la ley.

De allí la importancia de establecer políticas claras para la Entidad, que permitan proteger la Información y los datos personales, señalados en un solo acto administrativo, lo que permitirá establecer lineamientos actualizados estandarizando procesos y estableciendo ejercicios de aseguramiento de la Información, teniendo en cuenta los requisitos legales, operativos, tecnológicos, de seguridad con el fin de asegurar el cumplimiento de la integridad, disponibilidad, legalidad y confidencialidad de la información.

II. AMBITO DE APLICACIÓN Y SUJETO A QUIEN VA DIRIGIDO

Secretaría General, Directores de área, Jefes de Oficina de la Dirección General, Directores Regionales y Subdirectores de Centros de Formación Profesional del SENA.

Del mismo modo, la Política de Seguridad de la Información y protección de datos personales, aplica a todos sus funcionarios y contratistas que tengan acceso a información a través de cualquier medio con el que cuente la Entidad.



SERVICIO NACIONAL DE APRENDIZAJE SENA

FORMATO DE MEMORIA JUSTIFICATIVA

III. VIABILIDAD JURÍDICA	
1. Análisis de normas que otorgan competencia para la expedición del acto.	Artículo 76 de la Ley 489 de 1998. Funciones de los consejos directivos de los establecimientos públicos. Artículo 3 Decreto 249 de 2006. Funciones del Consejo Directivo Nacional. “1. Definir y aprobar la política general de la entidad y velar por su cumplimiento (...). 22. Aprobar la política nacional de calidad de la entidad, en el marco del Sistema de Gestión de Calidad institucional
2. La vigencia de la ley o norma reglamentada o desarrollada.	Artículo 76 de la Ley 489 de 1998, el artículo 3 del Decreto 249 de 2004, y el acuerdo 009 de 2016, citados en el acuerdo no han sido modificadas, derogadas, ni declaradas inexecutable o anuladas en los apartes invocados, por lo cual están vigentes y surtiendo efectos jurídicos.
3. Disposiciones derogadas, subrogadas, modificadas, adicionadas o sustituidas, estos efectos se producen con la expedición respectivo acto.	Con la expedición de este acuerdo, se derogar el acuerdo 009 de 2016, Por el cual se aprobó la Política del tratamiento para la Protección de Datos Personales en el Servicio Nacional de Aprendizaje (SENA).
4. Revisión y análisis de decisiones judiciales de los órganos de cierre de cada jurisdicción que pudieran tener impacto o ser relevantes para la expedición del acto.	Sentencia C-748 de 2011. ➤ Control constitucional al Proyecto de Ley Estatutaria No. 184 de 2010 Senado; 046 de 2010 Cámara, “por la cual se dictan disposiciones generales para la protección de datos personales” Sentencia C-1011/08 ➤ Revisión de constitucionalidad del Proyecto de Ley Estatutaria No. 27/06 Senado – 221/07 Cámara (Acum. 05/06 Senado) “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.
5. Otras circunstancias jurídicas relevantes para la expedición del acto.	El SENA no evidencia otra circunstancia jurídica relevante que advertir para la expedición del acuerdo.
IV. IMPACTO ECONÓMICO DE LA DECISIÓN	
La expedición del acuerdo no tendrá impacto económico para la Entidad.	
V. DISPONIBILIDAD PRESUPUESTAL	
La expedición del acuerdo no tienen afectación presupuestal.	
VI. IMPACTO MEDIOAMBIENTAL O SOBRE EL PATRIMONIO CULTURAL DE LA NACIÓN	
La expedición e implementación del acuerdo no genera impacto ambiental ni sobre el patrimonio cultural de la Nación.	



**SERVICIO NACIONAL DE APRENDIZAJE SENA
FORMATO DE MEMORIA JUSTIFICATIVA**

VII. CONSULTAS y PUBLICIDAD

1.Consulta previa: No se requiere, porque no hay norma Constitucional, Legal ni reglamentaria que así lo ordene.

2. Publicidad: en cumplimiento de lo dispuesto en el numeral 8 del artículo 8 de la Ley 1437 de 2011, y en concordancia con lo previsto en el artículo 2.1.2.1.14 del Decreto 1609 de 2015, el texto del presente acto administrativo se publicó en la página web del SENA para comentarios del público, entre el **xx** de **xxx** y el **xxx** de **xxx** de 201**x**. Las observaciones y sugerencias recibidas fueron debidamente analizadas e incorporadas de acuerdo con su pertinencia.

VIII. ASPECTOS ADICIONALES RELEVANTES

IX. RAZONES PARA EXPEDIR NUEVO ACTO E IMPACTO EN LA SEGURIDAD JURÍDICA

**X. SÍNTESIS DE LAS OBSERVACIONES Y COMENTARIOS DE LOS CIUDADANOS Y DE LOS GRUPOS DE INTERÉS
AL PROYECTO ESPECIFICO DE REGULACIÓN**

**XI. INFORME GLOBAL CON LA EVALUACIÓN POR CATEGORÍAS, DE LAS OBSERVACIONES Y COMENTARIOS
DE LOS CIUDADANOS Y GRUPOS DE INTERÉS**

En cumplimiento de lo dispuesto en el numeral 6 del artículo 3 de la Ley 1437 de 2011, en concordancia con del Decreto 270 de 2017, el informe global con la evaluación por categorías, posterior al vencimiento de participación ciudadana se publica en la sección de transparencia y acceso a la información se publica en la página web del SENA el **xx** de **xxx** de 201**x**.

**XII. EL PROYECTO CUMPLE CON LAS DIRECTRICES DE TÉCNICA NORMATIVA PREVISTAS EN EL DECRETO No.
1609 de 2015 Y EL DECRETO No. 270 DE 2017:**

SI _____ NO _____

XIII. ANEXOS



SERVICIO NACIONAL DE APRENDIZAJE SENA
FORMATO DE MEMORIA JUSTIFICATIVA

Vo. Bo. Director(a) Jurídico(a)

Revisó:

Proyectó: