ACUERDO 13 DE 2019

(diciembre 26)

Diario Oficial No. 51.238 de 25 de febrero 2020

SERVICIO NACIONAL DE APRENDIZAJE

Por medio del cual se aprueba la Política General de Seguridad de la Información y Protección de Datos Personales en el SENA, y se dictan otras disposiciones.

EL CONSEJO DIRECTIVO NACIONAL,

en uso de las facultades legales, en especial las que le confiere el numeral 1 y el parágrafo del artículo 10 de la Ley 119 de 1994, 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 119 de 1994, en el numeral 1 y parágrafo del artículo 10, contempla entre las funciones asignadas al Consejo Directivo Nacional del SENA: “1. Definir y formular la política general y los planes y programas de la entidad.” / “Parágrafo. El Consejo Directivo Nacional podrá delegar en el Director General y en los Consejos Regionales las funciones que estime convenientes”;

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, 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 número 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 de datos 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, dispone que "el objeto de la ley, 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 que "constituye el marco general de la protección del ejercicio del derecho de acceso a la información pública en Colombia";

Que el Decreto número 1081 de 2015, Único Reglamentario del Sector Presidencia de la República, compiló el Decreto número 103 de 2015, que reglamenta parcialmente la Ley 1712 de 2014, el cual establece los temas relacionados con la gestión de la información pública, 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;

Que el Decreto número 1078 de 2015, modificado por el Decreto número 1008 de 2018, en el artículo 2.2.9.1.1.3, 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 las normas vigentes, le compete a la Dirección de Planeación y Direccionamiento Corporativo del SENA, definir y liderar el almacenamiento, custodia, seguridad y disponibilidad de la información en medios electrónicos en el SENA";

Que mediante el Acuerdo número 009 de 2016, expedido por el Consejo Directivo Nacional del SENA, 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 la Política de Protección de Datos Personales;

Que el SENA, en calidad de entidad pública, adscrita al Ministerio del Trabajo, dispone de un marco legal aplicable conforme a las leyes vigentes y un marco 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, so pena de incurrir en las sanciones previstas en la ley;

Que la Norma Técnica NTC- ISO-IEC 27001 del 2013 contempla los lineamientos a tener en cuenta en el diseño de las políticas en las Tecnologías de la Información, Técnicas de Seguridad y Sistemas de Gestión de la Seguridad de la Información;

Que tanto el Comité Directivo del SENA y el Comité de Gestión y Desempeño Institucional, mediante Acta número 19 del 28 de mayo de 2019, aprobó emitir la Política General de Seguridad de la Información y Protección de Datos Personales en el SENA;

Que a través de documento CONPES 3975 del 8 de noviembre de 2019, se establece la Política Nacional para la transformación digital e inteligencia artificial;

Que el Plan Nacional de Desarrollo 2018-2022 “Pacto por Colombia, pacto por la equidad” reglamentado por medio de la Ley 1955 de 2019 en su artículo 147 señala: “(…), Las entidades estatales del orden nacional deberán incorporar en sus respectivos planes de acción el componente de transformación digital siguiendo los estándares que para este propósito defina el Ministerio de Tecnologías de la Información y las Comunicaciones. En todos los escenarios la transformación digital deberá incorporar los componentes asociados a tecnologías emergentes, definidos como aquellos de la Cuarta Revolución Industrial, entre otros. (…)”;

Que en cumplimiento de las disposiciones normativas antes citadas, aunado al 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 de propiedad del SENA por parte de la comunidad SENA y de terceros, se hace necesario 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;

Que mediante documento fechado 20 de diciembre de 2019, suscrito por la Secretaria General del SENA y Secretaria del Consejo Directivo Nacional, certifica que en sesión presencial del Consejo Directivo Nacional número 1571 del 4 de diciembre de 2019, fue aprobado el proyecto de Acuerdo de la “Política General de Seguridad de la Información y Protección de Datos Personales en el Servicio Nacional de Aprendizaje (SENA) y se dictan otras disposiciones”;

En mérito de lo expuesto,

ACUERDA:

ARTÍCULO 1o. Aprobar la Política General de Seguridad de la Información y Protección de Datos Personales en el Servicio Nacional de Aprendizaje (SENA).

Doctrina Concordante

Concepto SENA 71693 de 2022

CAPÍTULO I.

DISPOSICIONES GENERALES.

ARTÍCULO 2o. OBJETIVO. Determinar los lineamientos que permitan proteger la información y protección de los datos personales que adopta el Servicio Nacional de Aprendizaje (SENA), a través de acciones de aseguramiento de la información, teniendo en cuenta los requisitos legales, operativos, tecnológicos y de seguridad de la entidad, alineados con el contexto de direccionamiento estratégico y de gestión del riesgo, con el fin de asegurar el cumplimiento de la integridad, disponibilidad, legalidad y confidencialidad de la información.

La seguridad de la información y protección de datos personales es una prioridad para la Entidad

fijados en el Plan Estratégico Institucional, promoviendo buenas prácticas institucionales, aplicando controles que permitan el uso adecuado de la información en el logro de la misión, visión y objetivos transformacionales de la Entidad, por lo tanto, es responsabilidad de todos los funcionarios, contratistas, aprendices y personal vinculado velar por el continuo cumplimiento de las políticas definidas.

ARTÍCULO 3o. OBJETIVOS ESPECÍFICOS.

a) Proporcionar elementos que permiten a los gerentes públicos del SENA y demás funcionarios contribuir a la aplicación de controles para hacer seguimiento a la efectividad y aplicación de las políticas, principios y derechos, que se desarrollarán en el Manual de la Política General de Seguridad de la Información y Protección de Datos Personales en el Servicio Nacional de Aprendizaje (SENA), y que será parte integral de este Acuerdo.

b) Crear en la comunidad SENA una cultura de respeto de los derechos fundamentales referidos al buen nombre de los funcionarios y terceros, en el uso debido de la información utilizada o en bases de datos que sea para el cumplimiento de los fines que se encuentren facultados, basados en la ley y la normatividad vigente.

c) Apoyar a las dependencias de la entidad para la salvaguarda de la información y demás servicios tecnológicos propios del SENA y en el tratamiento de datos personales, con el propósito de proteger a la entidad de riesgos, ataques por virus, compromiso de los sistemas de red, los servicios y aspectos legales.

d) Establecer lineamientos y políticas de seguridad y privacidad de la información que definan las directrices formales de actuación en la Entidad.

e) 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.

f) Mantener actualizadas las políticas y procedimientos relacionados con la Seguridad y Privacidad de la Información.

g) 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.

h) 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.

i) 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.

j) 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.

k) 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.

l) Garantizar una adecuada gestión de incidentes, eventos o debilidades de seguridad de la información, reduciendo su impacto, propagación y duración.

m) Fortalecer el conocimiento y las habilidades en seguridad y privacidad de la información en la comunidad SENA.

n) Sensibilizar al personal de la entidad en el uso adecuado, la importancia y protección de los activos de información.

o) Definir, implementar, operar y mejorar continuamente el Modelo de Seguridad y Privacidad de la Información MSPI del SENA aumentando y manteniendo el nivel de madurez requerido por la entidad.

ARTÍCULO 4o. ALCANCE DE LA POLÍTICA. La Política General de Seguridad de la Información y Protección de Datos Personales es de obligatorio cumplimiento y aplica a todos los servidores públicos, trabajadores oficiales, contratistas, instructores, aprendices, proveedores, aspirantes y demás grupos de interés que accedan a la información del Servicio Nacional de Aprendizaje (SENA).

ARTÍCULO 5o. DECLARACIÓN DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES DEL SENA. 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 la información, el conocimiento generado y la protección de datos personales tienen una importancia primordial en el cumplimiento del Plan Estratégico Institucional.

La Dirección de Planeación y Direccionamiento Corporativo en coordinación con la Oficina de Sistemas y las áreas funcionales, en el ámbito de sus competencias, 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, contemplando los recursos necesarios para que las Políticas de Seguridad de la Información y de Protección de Datos Personales se integre a todos los procesos de la Entidad. Para el logro de este propósito es necesaria la participación activa de los diferentes actores.

ARTÍCULO 6o. PRINCIPIOS RECTORES PARA LA PROTECCIÓN DE DATOS PERSONALES Y DE SEGURIDAD DE LA INFORMACIÓN. La Política General de Seguridad de la Información y Protección de Datos Personales en el Servicio Nacional de Aprendizaje (SENA), como sus políticas complementarias, tendrá en cuenta la aplicación de los principios rectores consagrados en la Constitución Política de Colombia y normatividad vigente, entre los cuales están la legalidad, transparencia, finalidad, libertad, veracidad o calidad, de acceso y circulación restringida, seguridad, confidencialidad y los que apliquen según las disposiciones legales vigentes.

CAPÍTULO II.

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES.

ARTÍCULO 7o. Adoptar el Manual de Política General de Seguridad de la Información y Protección de Datos Personales en el Servicio Nacional de Aprendizaje, el cual hará parte integral del presente Acuerdo.

PARÁGRAFO. El Manual de la Política General de Seguridad de la Información y Protección de Datos Personales del SENA indica los lineamientos técnicos y operativos que apoyarán la gestión de la seguridad y privacidad de la información y protección de datos en la Entidad, permitiendo la integración del Sistema Integrado de Gestión y Autocontrol (SIGA) con el Subsistema de Seguridad de la Información, y llevando la implementación de los controles necesarios para salvaguardar la información del SENA desde la Dirección General hasta sus centros de formación.

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

Doctrina Concordante

Concepto SENA 62686 de 2020

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

a) Política de Clasificación y Manejo de Información. Asegura que los activos de información reciban un nivel de protección adecuado, clasificando, etiquetando y manejando la información del Servicio Nacional de Aprendizaje (SENA) de acuerdo con su valor, criticidad y requisitos legales que le aplique.

b) Política de adquisición, desarrollo y mantenimiento de sistemas de información. Establece las directrices y medidas de seguridad de la información, que se deben tener en cuenta durante el desarrollo de todas las actividades de adquisición, desarrollo y mantenimiento de sistemas de información en el Servicio Nacional de Aprendizaje (SENA).

c) Política de Control de Acceso. Establece las directrices y medidas de seguridad, que se deben tener en cuenta para otorgar, mantener y retirar los privilegios de acceso a los activos de información del Servicio Nacional de Aprendizaje (SENA).

d) Política de Criptografía. Establece los mecanismos que aseguren el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, disponibilidad, autenticidad y/o la integridad de la información del Servicio Nacional de Aprendizaje (SENA).

e) Política de cumplimiento de requisitos legales y contractuales. Garantiza el cumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad y privacidad de la información y de cualquier requisito de seguridad.

f) Política de Gestión de Incidentes de Seguridad de la Información. Establecer las directrices y

medidas de seguridad, que se deben tener en cuenta para la adecuada gestión de incidentes y debilidades de seguridad de la información que se identifiquen durante la prestación de los servicios de la Entidad y que puedan poner en riesgo los activos de información del Servicio Nacional de Aprendizaje (SENA).

g) Política de Relaciones con los Proveedores. Establece los lineamientos y medidas de seguridad de la información que se deben tener en cuenta en las relaciones que existan con proveedores de bienes, obras y/o servicios que, por el desarrollo de las funciones contratadas, tengan acceso a activos de información y a las instalaciones del Servicio Nacional de Aprendizaje (SENA).

h) Política de Seguridad de la Información en la Gestión de Continuidad del Negocio. Garantiza que los aspectos de Seguridad de la Información del Servicio Nacional de Aprendizaje (SENA) sean incluidos y contemplados en la Gestión de Continuidad de Negocio y en los eventos que requieran la activación de las estrategias de continuidad y/o contingencia de la Entidad.

i) Política de Seguridad de las Operaciones. Establece los lineamientos y medidas de seguridad, que se deben tener en cuenta dentro de las instalaciones de procesamiento de información, garantizando que se realicen en términos de seguridad y se garantice la protección de la información del Servicio Nacional de Aprendizaje (SENA).

j) Política de Seguridad de las Redes. Establece los lineamientos y medidas de seguridad, que se deben tener en cuenta para el diseño, implementación, operación, mantenimiento y demás labores relacionadas con los canales de comunicación de la Entidad de forma que se minimice la posibilidad de materialización de riesgos sobre los activos de información del Servicio Nacional de Aprendizaje (SENA).

k) Política de Seguridad Física y del Entorno. Protege las instalaciones físicas y de procesamiento de información del Servicio Nacional de Aprendizaje (SENA) contra acceso o intrusiones no autorizadas, de igual manera prevenir el hurto, alteración o pérdida de disponibilidad de los activos de la Entidad.

l) Política de Transferencia de Información. Establece los lineamientos y medidas de seguridad que se deben tener en cuenta para el diseño, implementación, operación, mantenimiento y demás labores relacionadas con los canales de comunicación de la Entidad, de forma que se minimice la posibilidad de materialización de riesgos sobre los activos de información del Servicio Nacional de Aprendizaje (SENA).

m) Política de Usuario Final. Establece las directrices de Seguridad y Privacidad de la Información que deben tener en cuenta los usuarios que tengan acceso y utilicen los activos de información del Servicio Nacional de Aprendizaje (SENA).

n) Política Gestión de Activos. Identifica y mantiene un inventario de todos los activos de información de los procesos incluidos dentro del alcance del Modelo de Seguridad y Privacidad de la Información (MSPI), del Servicio Nacional de Aprendizaje (SENA), teniendo en cuenta sus características, valor y responsabilidades sobre cada uno de ellos.

o) Política Seguridad de los Recursos Humanos. Establece los lineamientos que debe tener en cuenta el personal del Servicio Nacional de Aprendizaje (SENA) para comprender claramente sus responsabilidades en materia de Seguridad de la Información antes, durante y después de la vigencia del vínculo laboral o contractual con la entidad.

p) Política Seguridad de la Protección de Datos Personales. Esta política tendrá como propósito dar cumplimiento a las disposiciones constitucionales y legales para la salvaguarda de la información personal susceptibles de tratamiento por las entidades de naturaleza pública o privada.

PARÁGRAFO. Será el Director General del Sena a través de acto administrativo, quien apruebe y adopte las políticas complementarias necesarias para garantizar la implementación del Manual de Seguridad de la Información y Protección de Datos Personales en el SENA.

CAPÍTULO III.

RESPONSABILIDAD EN LA SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES.

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

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

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

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

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 las normas constitucionales, legales y reglamentarias.

ARTÍCULO 13. ENCARGADO DEL TRATAMIENTO DE DATOS PERSONALES. Delegar en el Director General del SENA la facultad de designar mediante resolución a un funcionario competente en la materia que se encargue del tratamiento de datos personales, quien deberá respetar y cumplir las condiciones de seguridad y privacidad de los titulares de la información.

ARTÍCULO 14. REVISIÓN. La Política General de Seguridad de la Información y Protección de Datos Personales será revisada anualmente o antes, en el caso que amerite su modificación. Este proceso será liderado por la Dirección de Planeación y Direccionamiento Corporativo, y será revisado y aprobado por el Comité Institucional de Gestión y Desempeño del Servicio Nacional de Aprendizaje (SENA).

ARTÍCULO 15. ARTÍCULO TRANSITORIO. Para los efectos de la aplicación del presente Acuerdo, se mantendrá vigente el Acuerdo número 009 de 2016 y su instructivo de Política de Protección de Datos Personales, mientras se desarrollan las Políticas Complementarias de Tratamiento de Datos Personales en la Entidad.

ARTÍCULO 16. COMUNICACIÓN. 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 y a la comunidad en general para su conocimiento y aplicación.

ARTÍCULO 17. VIGENCIA. El presente Acuerdo rige a partir de la fecha de su publicación en el Diario Oficial y deroga los demás actos administrativos que le sean contrarios, excepto el Acuerdo número 009 de 2016 que continuará vigente hasta que sea implementada la Política Complementaria que rige la materia. De conformidad con el principio de transparencia publíquese en la página web del SENA.

Publíquese, comuníquese y cúmplase.

Dado en Bogotá, D. C., a 26 de diciembre de 2019.

El Viceministro de Empleo y Pensiones, Presidente Consejo Directivo,

Andrés Felipe Uribe Medina.

La Secretaria General SENA, Secretaría del Consejo,

Verónica Ponce Vallejo.

MANUAL DE POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS

SENA

1. introducción

2. Gestión sobre las Políticas de Seguridad de la información y protección de Datos

3. Organización de Seguridad de la información

3.1 Roles y responsabilidades

3.2 Dispositivos móviles y teletrabajo

4 Seguridad de los Recursos Humanos

7 Seguridad de las Comunicaciones

7.1 Gestión de la seguridad de redes

7.2 Uso de la Mensajería Electrónica

7.3 Uso adecuado del servicio de Internet

7.4 Transferencia de Información

7.4.1 Políticas y procedimientos de transferencia o transmisión de información

8 Adquisición, Desarrollo y Mantenimiento de Sistemas

8.1 Requisitos de seguridad de los sistemas de información

8.2 Seguridad en los procesos de desarrollo y de soporte

8.2.1 Política de desarrollo seguro

8.3 Datos de prueba

8.3.1 Protección de datos de prueba

9 Relaciones con los Proveedores

9.1 Política de seguridad de la información para las relaciones con los proveedores

9.2 Gestión de la Prestación de Servicios de Proveedores

10 Gestión de Incidentes de Seguridad de la Información

10.1.1 Política de Administración de Acceso de Usuarios

10.1.2 Responsabilidades de acceso de los usuarios

10.1.3 Registro y cancelación del registro de usuario

10.2 Control de acceso a sistemas y aplicaciones

10.2.1 Restricción de acceso a la información

10.2.2 Procedimiento de Inicio de Sesión seguro

10.2.3 Sistema de gestión de contraseñas

10.2.4 Control de acceso a códigos fuentes de aplicaciones

11 Cifrado

11.1 Controles Criptográficos

11.1.1 Política sobre el uso de controles criptográficos

12 Seguridad Física y del Entorno

12.1 Áreas Seguras

12.1.1 Controles Físicos de Entrada

12.1.2 Protección sobre amenazas externas y ambientales

12.1.3 Trabajo en Áreas Seguras

12.2 Equipos

12.2.1 Ubicación y Protección de los Equipos

12.2.2 Seguridad del Cableado

12.2.3 Mantenimiento de Equipos

12.2.4 Equipos de usuarios desatendidos

12.2.5 Política de escritorio limpio y pantalla limpia

13 Seguridad de las Operaciones

13.1 Procedimientos operacionales y responsabilidades

13.1.1 Gestión de Cambios

13.1.2 Gestión de capacidades

13.1.3 Separación de Entornos de desarrollo, pruebas y producción

13.2 Gestión de incidentes y mejoras en la seguridad de la información

13.2.1 Responsabilidades y procedimientos

14 Aspectos de Seguridad para la Gestión de Continuidad de Negocios

14.1 Continuidad de Seguridad de la Información

15 Cumplimiento

15.1 Cumplimiento de requisitos legales y contractuales

15.1.1 Identificación de la legislación aplicable y de los requisitos contractuales

15.1.2 Privacidad y protección de información de datos personales

15.2 Revisiones de seguridad de la información

15.2.1 Cumplimiento con las políticas de seguridad de la Información

16 Política de Privacidad y Protección de datos personales

16.1.1 Marco Legal

16.2 Principios Rectores

16.3 Categorías Especiales de Datos

1 Introducción

El Servicio Nacional de Aprendizaje - SENA, implemento mediante el Acuerdo XXX de 2019, la política general de seguridad de la información y protección de datos personales, dando cumplimiento a los principios de integridad, confidencialidad y disponibilidad de la información, determinando los lineamientos que permitan proteger la Información y protección de los datos personales que adopte la Entidad, 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; para lo cual diseñará e implementará los controles de seguridad que reduzcan los riesgos de perdida y vulnerabilidad de la misma, por agentes internos y/o externos a la Entidad.

Para el cumplimiento de este propósito se emite el manual de políticas de seguridad de la información y protección de datos personales, que tiene como propósito conservar la integridad, confidencialidad y disponibilidad de la información, como la de velar porque los responsables del tratamiento de datos personales y de la información del SENA generen y adopten las respectivas políticas que abarquen el cumplimiento de los mandatos constitucionales y legales

para salvaguardar la misma.

Con este manual se formaliza el compromiso de la Alta Dirección frente a la gestión de la seguridad de la información que reposa en el SENA y presenta de manera escrita - en lenguaje claro y sencillo- para que los usuarios comprendan el compendio de acciones que se implementarán para proteger de posibles riesgos de daño, pérdida y uso indebido de la información, cuidado los equipos y demás recursos informáticos de la Entidad.

El SENA a través de la Dirección de Planeación y Direccionamiento Corporativo en coordinación con La Oficina de Sistemas o quien haga sus veces, divulgará y socializará las políticas y procedimientos de seguridad de la información y las que se deriven de esta, con el fin de que los usuarios SENA y partes interesadas, es decir, todas las personas u organizaciones tanto públicas o privadas, internas o externas, que de alguna manera quieran interactuar con el SENA, adopten una postura de seguridad, para proteger la información y evitar su divulgación no autorizada.

El presente manual resguarda los siguientes dominios de seguridad de la Información los cuales se describen claramente en el desarrollo de todo el documento.

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

2 Gestión sobre las Políticas de Seguridad de la Información y protección de Datos

- El SENA a través de la Dirección de Planeación y Direccionamiento Corporativo, en atención a la competencia que le asiste, emitirá lineamientos para la gestión de la seguridad de la información, a través de los cuales se velará por la administración de seguridad, implementación, funciones y responsabilidades; adicionalmente en coordinación con la Oficina de Sistemas o quien haga sus veces, se implementarán las medidas de seguridad necesarias para la protección y manejo de la información de la entidad.

- La Dirección de Planeación y Direccionamiento Corporativo en coordinación con La Oficina de Sistemas o quien haga sus, realizarán las gestiones necesarias para que este manual y las políticas complementarias sean comunicadas y aplicadas en el SENA; así mismo, será revisado anualmente, o antes en el caso que amerite su modificación; este trámite será liderado por la Dirección de Planeación y Direccionamiento Corporativo.

- El subsistema de seguridad de la información de la entidad contemplará los diferentes dominios de seguridad expuestos en el presente manual y será gestionado por la Dirección de Planeación y Direccionamiento Corporativo en coordinación con La Oficina de Sistemas o quien haga sus veces.

3 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 (chief information security officer), entendido como el Oficial de Seguridad de la Información, o quien haga sus veces de la Dirección de Planeación y Direccionamiento Corporativo; deberá 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.

- El SENA propenderá por la generación y mantenimiento de un equipo interdisciplinario dedicado a seguridad de la información, seguridad informática y protección de datos personales; el cual velará por el eje de seguridad del SENA. Para la conformación de este equipo se tendrá en cuenta las fases de desarrollo de la política que conlleven a su implementación durante el año 2020.

- La Dirección de Planeación y Direccionamiento Corporativo en coordinación con La Oficina de Sistemas o quien haga sus veces, velarán por el mantenimiento del Sistema de Gestión de la Seguridad de la Información (SGSI), con el fin de garantizar la ejecución de controles y seguimiento a los mismos.

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

3.1 Roles y responsabilidades

Propietario: El SENA es propietario de los activos de información, para lo cual debe clasificar la información, establecer el nivel de criticidad y disponibilidad de esta.

Responsable: Los directores de área y jefes de oficina de la dirección general, directores regionales y subdirectores de centro de formación profesional integral, son responsables de asegurar la información de su dependencia, quienes velarán por que se cumplan los requerimientos de seguridad señalados en este manual o en las políticas complementarias y/o los procedimientos de seguridad y medidas implementadas por el custodio.

La Dirección de Planeación y Direccionamiento Corporativo definirá los lineamientos y liderará el almacenamiento, custodia, seguridad y disponibilidad de la información en medios electrónicos en el SENA.

La Oficina de Sistemas o quien haga sus veces implementará las medidas y controles necesarios para salvaguardar los activos de información de acuerdo con la clasificación establecida por los propietarios.

Custodio: Se define como custodio a la Dirección de Planeación y Direccionamiento Corporativo, quien administrará y hará efectivos los controles de seguridad que el propietario de la información haya definido.

Usuario: Los servidores públicos, aprendices, contratistas, entidades públicas o privadas y toda aquella persona que se conecte a la red del SENA o utilice los activos de información, deben hacer un buen uso del acceso a la información que se le suministre y cumplir con las políticas de seguridad dadas a través de este manual.

3.2 Dispositivos móviles y teletrabajo

- Los equipos o dispositivos móviles que hagan uso de la información del SENA o que se conecten a sus redes, deben acoger las políticas de seguridad de la información y protección de datos personales, 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 o quien haga sus veces, debe disponer de los procedimientos y mecanismos de conexión para el uso de la información y los servicios tecnológicos del SENA en dispositivos móviles tanto de propiedad del SENA, como de propiedad de terceros.

- La Oficina de Sistemas o quien haga sus veces, debe disponer de mecanismos de conexión seguros que garanticen el correcto acceso a través de los canales que se dispongan para la modalidad de teletrabajo en el SENA, de manera que se protejan los activos de información en uso, para lo cual se deben garantizarán los recursos.

4 Seguridad de los Recursos Humanos

4.1 Antes de la contratación (asumir el Empleo)

La Secretaría General desde donde se gestiona el proceso estratégico de talento humano, deberá emitir una guía o lineamientos que permitan verificar el cumplimiento de requisitos para acceder a los empleos, y así mismo dejar claro los roles y responsabilidades junto con el acceso a la información que tendrá el personal de la planta permanente y temporal, bien sea de manera definitiva o transitoria, conforme lo establezca el Manual de Funciones vigente.

Adicional a lo anterior las áreas encargadas de la contratación de la dirección general, regionales y centro de formación del SENA, incluirán en la documentación de los contratos un acuerdo de confidencialidad.

4.2 Durante el ejercicio de roles (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) y del Sistema de Gestión de Seguridad de la Información - SGSI, 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 velar por la implementación y el cumplimiento de la política de seguridad de la información y protección de datos personales y políticas complementarias que se generen.

- 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.

- Para el caso de los servidores públicos (vinculados a la planta de personal([1])), el equipo directivo y jefes inmediatos pondrá en conocimiento de la Oficina de Control Interno o de la autoridad competente (penal o fiscal, según el caso), las posibles violaciones o incidentes de seguridad de la información que así lo ameriten.

- Para el caso de los aprendices estará basado en el reglamento del aprendiz y se debe poner en conocimiento de las autoridades penales y/o fiscales, según sea el caso, cuando se identifiquen el uso indebido de la información y datos personales que reposen en las bases de datos y/o documentos SENA. Para los contratistas, cuando se identifiquen violaciones o incidentes de seguridad en el que hagan uso indebido de la información y datos personales que reposen en las bases de datos y/o documentos SENA, el supervisor realizara el procedimiento por incumplimiento definido en la normatividad vigente y en la cláusula contractual y se debe poner en conocimiento de las autoridades penales y/o fiscales, según sea el caso.

- La Dirección de Planeación y Direccionamiento Corporativo, en conjunto con la Oficina de Sistemas o quien haga sus veces, serán los encargados de convocar a los directivos, servidores públicos, contratistas, aprendices a las sensibilizaciones, charlas, talleres y/o 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 control.

- Los aprendices que en etapa lectiva o en desarrollo del contrato de aprendizaje, 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 en seguridad de la información.

- Toda la comunidad SENA, se abstendrá de divulgar información confidencial de la Entidad, de manera escrita o verbal; de la misma manera, aplica para situaciones donde la revelación de información pueda causar un impacto operativo o repercusiones legales para el SENA.

4.3 Cambio funcional o de empleo, retiro y/o terminación de otros tipos de vinculación

El Sena velara porque se mantengan los criterios de seguridad dados a través de este manual, al momento de realizar procesos de cambios de funciones, de empleo, de retiro, de finalización del contrato, desvinculación y/o retiro; actividades que se harán de forma ordenada, controlada y segura, tanto para servidores públicos como contratistas.

5 Gestión de Activos

5.1 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 que se proporcionan a los funcionarios, contratistas, aprendices y a terceros autorizados, para cumplir con los propósitos institucionales.

- Todos los activos del SENA previa asignación a un responsable deben estar inventariados y clasificados de acuerdo con los requerimientos y los criterios que se parametrizaron en la guía de clasificación de activos de la información.

5.1.1 Responsables de los Activos de Información

El Director General, Secretaría General, los directores de área, Jefes de Oficina, Directores Regionales, Subdirectores de Centro y Coordinadores de Grupo, deben actuar como responsables de la información física y electrónica de las dependencias a cargo y en ejercicio de sus facultades deberán:

- Aprobar o revocar el acceso a su información con los perfiles adecuados.

- Generar el inventario de los activos para los grupos 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.

- Monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información cada seis meses.

- Utilizar los recursos tecnológicos de la entidad solo para la realización de sus labores asignadas al cargo; por consiguiente, no deben ser utilizados para fines ajenos a este.

- El Director General, Secretaría General, los directores de área, Jefes de Oficina, Directores Regionales, Subdirectores de Centro y Coordinadores de Grupo y, aprendices que requieran utilizar equipos propios diferentes a los proporcionados por la institución, deben solicitar la autorización, verificación y registro de la Oficina de Sistemas o quien haga sus veces.

- La Oficina de Sistemas o quien haga sus veces, 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 aprendices deben utilizar los recursos tecnológicos del SENA (laboratorios de cómputo, servicios web y otros) para provecho de la formación educativa, por consiguiente, no deben ser utilizados para fines ajenos a este.

- Todo el personal del SENA y terceros deben cumplir con los controles mínimos de seguridad establecidos por la Oficina de Sistemas o quien haga sus veces, para poder conectarse a la red del SENA (antivirus, sistema operativo con actualizaciones de seguridad, entre otros).

- Todo el personal del SENA y terceros, cuando requiera instalar, hacer uso o compartir software (libre o propio) en los recursos proporcionados por la entidad, deben solicitar a la Oficina de

Sistemas o quien haga sus veces la autorización, verificación y registro.

- Todo el personal del SENA en el momento de un cambio funcional o de empleo, retiro y/o terminación de otros tipos de vinculación, 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 durante su permanencia en la Entidad.

- La Oficina de Sistemas o quien haga sus veces, 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 o autorizado.

5.2 Clasificación de la Información

- El SENA definirá la clasificación de la información con los niveles de seguridad de acuerdo con la normatividad vigente y al grado de sensibilidad identificada; la Dirección de Planeación y Direccionamiento Corporativo en acompañamiento de la Oficina de Sistemas o quien haga sus veces generará una guía de clasificación de la información, la cual deberá ser aplicada por los propietarios quienes procederán a catalogarla y determinarán 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 de niveles de seguridad define los controles técnicos y administrativos que se aplicarán en la entidad, con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos en función de su nivel de clasificación.

5.2.1 Clasificación y Manejo de la Información

Todo el personal del SENA debe cumplir con los lineamientos establecidos en el manual de clasificación de la Información atendiendo los niveles de seguridad 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 Secretaría General a través del Grupo Administración de Documentos debe tener un periodo de almacenamiento para la información física y digital, de acuerdo con lo establecido en las Tablas de Retención Documental y los procedimientos establecidos normativamente para la disposición final.

- El personal del SENA, cuando imprima, escanee y/o utilicen medios reprográficos, deben tener en cuenta:

- Luego de escanear, fotocopiar o utilizar un medio reprográfico debe asegurarse de no dejar documentos en los equipos utilizados.

- Recoger de las impresoras, escáneres, fotocopiadoras y/o medios reprográficos, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.

- Asegurarse que los documentos y medios de almacenamiento que contengan información sensible no queden de forma desprotegida en el momento de ausentarse de su puesto de trabajo.

- Proteger la información física de la entidad, utilizando los medios de almacenamiento y resguardo de los que dispongan.

Para dar cumplimiento con la clasificación de la información de niveles de seguridad se presentan los tipos de prioridad de acuerdo con la siguiente clasificación:

- Pública: estará la información que se puede compartir.

- Uso interno: estará la información de interés para la entidad, en general.

- Confidencial: estará la información de interés solo para un área en particular o por disposición de la ley (datos sensibles, privados, menores de edad, etc.).

- Para el tratamiento de datos deberá tenerse en cuenta las normas constitucionales y legales vigentes y las que reglamenten la materia.

- El Director General, Secretaría General, los directores de área, Jefes de Oficina, Directores Regionales, Subdirectores de Centro y Coordinadores de Grupo deben realizar la entrega de toda la información que durante el ejercicio del cargo, recibieron, produjeron o administraron independientemente del soporte que la contenga a quien lo suceda en el cargo.

- El Director General, Secretaría General, los directores de área, Jefes de Oficina, Directores Regionales, Subdirectores de Centro y Coordinadores de Grupo deben garantizar la conservación de la información sin importar el soporte que la contenga.

- La información clasificada de la entidad únicamente podrá ser consultada o gestionada por el personal autorizado, para el desarrollo de sus funciones y no para usos propios o ajenos a la entidad.

- El personal del SENA o terceros no deberá usar o sustraer material o información confidencial y/o reservada de la entidad, para usos ajenos a sus funciones.

5.2.2 Etiquetado de la Información

Cada activo de información debe poseer un etiquetado donde se identifique el nivel de la clasificación asignado, de igual manera esta información debe ser documentada. Esta etiqueta debe ser utilizada para la información que se encuentre en medio físico como digital.

El Director General, la Secretaría General, los directores de área, Jefes de Oficina, Directores Regionales, Subdirectores de Centro y Coordinadores de Grupo son responsables de la información contenida en las unidades a su cargo por lo cual, deben tomar e implementar las medidas de seguridad necesarias para salvaguardar la información.

5.3 Manejo de medios de Almacenamiento

- El SENA evitará la divulgación no autorizada, la modificación, eliminación o destrucción de la información en los medios de almacenamiento dispuestos para tal fin, para lo cual se diseñarán las políticas complementarias que conlleven a la mitigación de riesgos en el manejo de la información.

- Para el diseño, desarrollo e implementación de las políticas para el manejo de la información en los medios de almacenamiento se hará de manera articulada con los demás sistemas de gestión de la Entidad.

5.3.1 Gestión de medios extraíbles

- La Oficina de Sistemas o quien haga sus veces, 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.

- Los equipos de cómputo que tienen autorizado el manejo de medios extraíbles tales como Tarjetas de memoria USB, SD y unidades reproductoras de CD/DVD, deben cumplir mínimo con los siguientes requisitos:

- Tener habilitado el escaneo automático de virus.

- Tener configurado el bloqueo de la reproducción automática de archivos ejecutables a través del antivirus o por otro medio.

- Los dispositivos de almacenamiento de información de propiedad del SENA se constituyen un activo de información, por lo tanto el ingreso, uso, movilización y salida debe realizarse siguiendo los lineamientos para este fin.

5.3.2 Eliminación de información en los Medios

De acuerdo con los procedimientos establecidos en las normas vigentes y las tablas de retención Documental la Oficina de Sistemas o quien haga sus veces debe velar porque la información sea eliminada de los medios de almacenamiento, atendiendo los ciclos de vida de los activos de información, para lo cual deberá utilizar herramientas de borrado seguro garantizando que no queden rastros de esta.

5.3.3 Medios físicos e Información en tránsito

- La Oficina de Sistemas o quien haga sus veces, debe velar que los medios que contienen información clasificada estén protegidos contra acceso no autorizado, mal uso o corrupción durante el transporte.

- La Oficina de Sistemas o quien haga sus veces, debe velar que la información que transita a través de la red cuente con los protocolos de seguridad necesarios, asegurando su confidencialidad, disponibilidad e integridad.

- La Oficina de Sistemas o quien haga sus veces, debe implementar la utilización de protocolos de seguridad para el cifrado de los datos.

6 Control de Acceso

6.1 Política de Control de Acceso

- La Entidad garantizará entornos con controles de acceso idóneos, los cuales aseguren el perímetro, tanto en la dirección general, regionales, centro de formación y sedes, así como en entornos abiertos para evitar el acceso no autorizado a ellos.

- Así mismo, controlará las amenazas físicas externas y velará por proveer las condiciones

medioambientales requeridas para el funcionamiento de la plataforma tecnológica y para la preservación de sus activos de información digitales y físicos.

- La Oficina de Sistemas o quien haga sus veces, debe asegurar la implantación y efectividad de mecanismos de seguridad física, controles de acceso físico y condiciones medioambientales con los que se debe contar.

- Los proveedores responsables de las áreas seguras tienen la obligación de vigilar y garantizar que se cumplan las siguientes medidas de seguridad:

- Las áreas que se catalogan como seguras deben permanecer cerradas y custodiadas.

- El acceso a áreas seguras donde se procesa o almacena información confidencial, de uso interno y público, es limitado únicamente a personas autorizadas.

6.1.1 Acceso a Redes y a Servicios en Red

- La Oficina de Sistemas o quien haga sus veces, como responsable de las redes de datos y los recursos de red de la entidad, debe velar porque dichas redes sean debidamente protegidas contra accesos no autorizados por medio de mecanismos de control de acceso lógico para lo cual deberá:

- Establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de la entidad.

- Asegurar que las redes inalámbricas cuenten con mecanismos de autenticación que evite los accesos no autorizados.

- Establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes a las redes o recursos de red del SENA, así como velar por la aceptación de las responsabilidades de dichos terceros en cuanto a las Políticas de Seguridad de la Información.

- Suministrar una herramienta para realizar conexiones remotas a la red de área local de la entidad de manera segura para todo el personal del SENA y terceros que por su labor así lo requiera, la cual debe ser aprobada, registrada y auditada.

- Tener implementado un procedimiento de creación de cuentas, donde estén definidas las condiciones de autorización y acuerdos de confidencialidad respectivos.

- La comunidad SENA y los terceros deberán:

- Suscribir un acuerdo de confidencialidad firmado, otorgado por el grupo de relaciones laborales o quien haga sus veces y la autorización de creación de cuentas otorgado por el jefe inmediato o quien haga sus veces, para tener acceso lógico a los sistemas de información de la entidad, según sea el caso.

- Cumplir los requisitos o controles de autenticación, cuando deseen que los equipos de cómputo personales accedan a la red de datos de la Entidad y solamente podrán utilizarlas para las tareas autorizadas.

6.1.2 Control de Accesos Remotos

Todo el personal del SENA, aprendices y terceros deben contar con una autorización y con los

mecanismos permitidos por la Oficina de Sistemas o quien haga sus veces, para realizar una conexión remota a equipos conectados a la red interna desde fuera de la misma.

6.2 Gestión de Acceso de Usuarios

6.2.1 Política de Administración de Acceso de Usuarios

- El SENA, establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la Entidad. Así mismo, el Director General, Secretaría General, los directores de área, Jefes de Oficina, Directores Regionales, Subdirectores de Centro y Coordinadores de Grupo tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

- La Oficina de Sistemas o quien haga sus veces, debe establecer un procedimiento formal para la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información de la Entidad; que contemple la creación, modificación, bloqueo, inactivación y/o eliminación de las cuentas de usuario.

- El Director General, Secretaría General, los directores de área, Jefes de Oficina, Directores Regionales, Subdirectores de Centro y Coordinadores de Grupo deben gestionar la creación, modificación, bloqueo, inactivación y/o eliminación de los usuarios y permisos a los diferentes sistemas de información y recursos tecnológicos ante la Oficina de Sistemas o quien haga sus veces, de quien será el encargado de ejecutar las labores a nivel tecnológico.

- La Oficina de Sistemas o quien haga sus veces, debe definir los lineamientos para las características que deben contener las contraseñas que se aplicarán sobre la plataforma tecnológica, los servicios de red y los sistemas de información.

- La Oficina de Sistemas o quien haga sus veces, debe establecer un procedimiento que asegure la inactivación y/o eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna.

- La Oficina de Sistemas o quien haga sus veces, debe asegurar que los usuarios o perfiles de usuario, que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica sean inhabilitados y/o eliminados.

- La Oficina de Sistemas o quien haga sus veces, en conjunto con los propietarios de los activos de información deben autorizar la creación o modificación de las cuentas de acceso de los recursos tecnológicos y sistemas de información de la entidad, según sea el caso.

- Los propietarios de los activos de información deben verificar y ratificar periódicamente (cada seis meses) todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

6.2.2 Responsabilidades de acceso de los usuarios

Los usuarios de los recursos tecnológicos y de los sistemas de información, realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual se les ha permitido el acceso.

6.2.2.1 Pautas de responsabilidad de acceso

Los funcionarios, contratistas, instructores, aprendices y terceros que hacen uso de la plataforma tecnológica, los servicios de red y los sistemas de información de la entidad, deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.

Ninguna persona debe compartir sus cuentas de usuario y contraseñas asignados para el ingreso a los servicios de red y los sistemas de información con otros miembros de la entidad o terceros.

Los funcionarios, contratistas, instructores, aprendices y terceros que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información que la entidad provee deben acogerse a las normas establecidas para la configuración de contraseñas designadas por la Entidad.

6.2.3 Registro y cancelación del registro de usuario

La Oficina de Sistemas o quien haga sus veces, debe crear un proceso formal de usuarios para asignar o revisar los derechos de acceso para todo tipo de usuarios, para todos los sistemas y servicios. (Usuarios y Roles).

La administración y gestión de los Usuarios en todos los Sistemas de Información / Aplicación del SENA, debe ser realizada por el área funcional quien, en el conocimiento del negocio, la información, procesos sensibles y niveles de autoridad debe asignar los privilegios teniendo en cuenta las funciones y el rol de cada uno de sus usuarios en el sistema.

6.3 Control de acceso a sistemas y aplicaciones

6.3.1 Restricción de acceso a la información

- Todo el personal del SENA y terceros serán responsables por las credenciales (usuario y contraseña) que le sean asignadas y que reciben para el uso y acceso de los recursos.

- Ningún usuario (funcionarios, contratistas, instructores, aprendices y terceros) recibirá credenciales de acceso a las plataformas tecnológicas, los servicios de red y los sistemas de información o aplicaciones, hasta que no acepte formalmente la Política de Seguridad de la Información vigente.

- Todos los funcionarios, contratistas, instructores, aprendices y terceros deberán autenticarse a través de los mecanismos de control de acceso provistos por la Oficina de Sistemas o quien haga sus veces, antes de poder usar la infraestructura tecnológica de la Entidad.

- Los funcionarios, contratistas, instructores, aprendices y terceros no deben proporcionar información de los mecanismos de control de acceso en las instalaciones e infraestructura tecnológica de la Entidad a personal externo, a menos que se tenga el visto bueno del propietario de la información, de la Oficina de Sistemas o quien haga sus veces y de su jefe inmediato.

- Los funcionarios, contratistas, instructores, aprendices y terceros, que accedan a la infraestructura tecnológica de la entidad, deben contar con un identificador de usuario (ID) único, personalizado e intransferible.

6.3.2 Procedimiento de inicio de Sesión seguro

- La Oficina de Sistemas o quien haga sus veces, debe asegurarse que el acceso a los servicios de

información solo sea posible con un proceso de conexión segura.

- La Oficina de Sistemas o quien haga sus veces, debe implementar los controles necesarios para proteger los servicios de información de intentos de inicio de sesión mediante ataques de fuerza bruta.

- La Oficina de Sistemas o quien haga sus veces, debe generar mensajes de advertencia general indicando que solo los usuarios autorizados pueden acceder al equipo de cómputo.

- La Oficina de Sistemas o quien haga sus veces, debe validar la información de ingreso a los servicios tecnológicos solamente al completar todos los datos de entrada. Si presenta una condición de error, el sistema no debe indicar qué parte de los datos es correcta o incorrecta.

- La Oficina de Sistemas o quien haga sus veces, debe habilitar el registro de los intentos exitosos y fallidos de acuerdo con los perfiles de los usuarios en los sistemas de información necesarios.

- La Oficina de Sistemas o quien haga sus veces, debe garantizar la transmisión segura de contraseñas sobre la red.

- La Oficina de Sistemas o quien haga sus veces, debe asegurar la terminación de sesiones inactivas después de un período de inactividad de cinco minutos, teniendo especial cuidado con lugares de alto riesgo, tales como áreas públicas o externas por fuera de la organización o en dispositivos móviles.

6.3.3 Sistemas de gestión de contraseñas

- Los funcionarios, contratistas, instructores, aprendices y terceros deben recibir junto con el nombre de usuario una contraseña o clave para acceder a los recursos informáticos de la Entidad, la cual es de cambio obligatorio en el primer uso, garantizando así su responsabilidad y único conocimiento sobre la misma.

- Los funcionarios, contratistas, instructores, aprendices y terceros deben establecer una contraseña que debe tener una longitud mínima de ocho caracteres alfanuméricos (mayúsculas, minúsculas, números, símbolos), diferentes a nombres propios o cualquier otra palabra de fácil identificación.

- Los funcionarios, contratistas, instructores, aprendices y terceros deben cambiar las contraseñas claves de acceso a la red, a los sistemas de información y demás con una periodicidad de 90 días.

- La Oficina de Sistemas o quien haga sus veces, debe cambiar las contraseñas o claves de Administrador de los diferentes sistemas con una periodicidad de 90 días.

- La Oficina de Sistemas o quien haga sus veces, debe establecer los controles necesarios para que después de tres intentos no exitosos al digitar la contraseña del usuario, esta se bloquee de manera inmediata y se deberá solicitar el desbloqueo en la plataforma destinada para este fin.

- Los funcionarios, contratistas, instructores, aprendices y terceros deben realizar su cambio de contraseña exclusivamente en la plataforma destinada para tal fin. No se podrán modificar por ningún otro medio.

- La Oficina de Sistemas o quien haga sus veces, debe asegurar que el número de sesiones

concurrentes de un mismo usuario sea limitado.

- La Oficina de Sistemas o quien haga sus veces, debe asegurar que el usuario sea usado en el equipo que fue asignado respectivamente.

- La Oficina de Sistemas o quien haga sus veces, debe establecer mecanismos para que las contraseñas o claves no sean iguales al nombre de usuario o cualquier variación (al revés, mayúsculas, etc.), alias o sobrenombre de la persona.

- Los funcionarios, contratistas, instructores, aprendices y terceros deben asegurarse de que la contraseña o clave no contiene palabras frecuentemente usadas y que se puedan asociar de manera rápida con su vida personal (nombre de hijos, fecha de nacimiento, número de cédula, número de celular, entre otros), no usa patrones como secuencias de números o caracteres y cadena repetidas.

- La Oficina de Sistemas o quien haga sus veces, debe proporcionar los mecanismos necesarios para que los funcionarios, contratistas, instructores, aprendices y terceros que olviden, bloqueen o extravíen su contraseña, puedan restablecerla de forma segura.

- Los funcionarios, contratistas, instructores, aprendices y terceros deben asegurarse de que las contraseñas no se encuentren de forma legible en cualquier medio impreso o digital ni dejarlos en un lugar donde personas no autorizadas puedan identificarlos.

- Los funcionarios, contratistas, instructores, aprendices y terceros deben cambiar inmediatamente la contraseña si tiene la sospecha de que esta es conocida por otra persona.

- Los funcionarios, contratistas, instructores, aprendices y terceros como usurarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad a menos que sea aprobada por la Oficina de Sistemas o quien haga sus veces.

6.3.4 Control de acceso a códigos fuentes de aplicaciones

- La Oficina de Sistemas o quien haga sus veces, debe implementar los controles necesarios para asegurar que el acceso al código fuente de los aplicativos desarrollados (sistemas de información) sea limitado. Solamente el personal autorizado podrá contar con acceso a esta información y hará un uso moderado de la misma.

- La Oficina de Sistemas o quien haga sus veces, debe proporcionar las herramientas necesarias para realizar control de cambios sobre el código fuente de los aplicativos desarrollados por la misma, las cuales permitirán retroceder a una versión anterior del código.

- La Oficina de Sistemas o quien haga sus veces, debe ser responsable por la aprobación, supervisión y modificación de los códigos fuente de los aplicativos.

7 Cifrado

7.1 Controles Criptográficos

El SENA, asegurará el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información clasificada de la Entidad al momento de almacenarse o transmitirse.

7.1.1 Política sobre el uso de controles criptográficos

- El Sena deberá asegurar el uso apropiado y eficaz de la Criptografía para proteger la confidencialidad, la autenticidad e integridad de la información. La Oficina de Sistemas o quien haga sus veces, deberá:

- Proporcionar los mecanismos o herramientas necesarias para asegurar la protección de claves de acceso a la red de datos, los sistemas de información, datos y servicios de la Entidad.

- Proporcionar los mecanismos de cifrado necesarios para asegurar que la transmisión de información clasificada de forma interna o externa se realice de forma segura.

- Proporcionar los mecanismos o herramientas necesarias para cifrar la información clasificada de la institución, resguardada por los propietarios de la información (funcionarios, contratistas, instructores, aprendices).

- Contar con una política para garantizar la privacidad de la información que se respalda en medios de almacenamiento secundarios. De manera que se recomienda cifrar dicha información para mayor seguridad.

8 Seguridad Física y del Entorno

8.1 Áreas Seguras

El SENA 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.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

8.1.1 Controles Físicos de Entrada

- Toda persona, que tenga acceso a las instalaciones del SENA, deberá registrar los equipos de cómputo que no sean de propiedad de la entidad, en la plataforma web establecida y de acuerdo a los procedimientos definidos por la Oficina de Sistemas o quien haga sus veces.

- Los funcionarios, contratistas, instructores, aprendices y terceros, que requieran ingresar a los centros de cómputo y a los centros de cableado, deben realizar las solicitudes de acceso a la Oficina de Sistemas o quien haga sus veces. En el caso de los centros de cómputo de la Oficina de Sistemas o quien haga sus veces, laboratorios y si existiesen otros centros similares, a la dependencia responsable del mismo. Adicional, los responsables deben realizar un registro del ingreso de los visitantes en una bitácora ubicada en la entrada de estos lugares de forma visible.

- Los funcionarios, contratistas, instructores, aprendices y terceros que deseen ingresar a los centros de cómputo y a los centros de cableado deben realizar el ingreso acompañados de un funcionario de la dependencia responsable de los mismos.

- Los funcionarios, contratistas, instructores, aprendices y terceros deben cumplir completamente con los controles físicos implementados por la Entidad, ya que los ingresos y salidas de las instalaciones del SENA deben ser registrados.

- Todo el personal del SENA y terceros deben portar el carné que los identifica como tal, en un

lugar visible, mientras se encuentren en las instalaciones de la Entidad; en caso de pérdida del carné, deben reportarlo a la mayor brevedad posible.

- Los funcionarios, contratistas, instructores, aprendices y terceros no deben intentar ingresar a las áreas a las cuales no tengan autorización.

- Las dependencias que tienen bajo su custodia centros de cómputo y centros de cableado deben modificar de manera inmediata los privilegios de acceso físico a estos sitios, en situaciones de cambio funcional o de empleo, retiro y/o terminación de otros tipos de vinculación.

- Las dependencias que tienen bajo su custodia centros de cómputo y centros de cableado deben velar por las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en estos sitios. Para cumplir con esto deben existir:

- Sistemas de control ambiental de temperatura y humedad
- Sistemas de extinción de incendios
- Sistemas de vigilancia y monitoreo

- Alarmas en caso de detectarse condiciones ambientales inapropiadas.

- Las dependencias que tienen bajo su custodia centros de cómputo y centros d cableado, en conjunto con la Dirección Administrativa y Financiera, deben velar porque los recursos de la plataforma tecnológica, ubicados en estos sitios, se encuentren protegidos contra fallas o interrupciones eléctricas.

- Las dependencias que tienen bajo su custodia centros de cómputo y centros de cableado, en conjunto con la Dirección Administrativa y Financiera, deben certificar que estos sitios se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

- Las dependencias que tienen bajo su custodia centros de cómputo y centros de cableado, en conjunto con la Dirección Administrativa y Financiera, deben asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y previamente autorizado e identificado.

- Las dependencias que tienen bajo su custodia centros de cómputo y centros de cableado deben llevar control de la programación de los mantenimientos preventivos a estos sitios, teniendo en cuenta los niveles de servicio acordados con los responsables de los servicios particulares y acorde a la operación de la entidad.

- Las dependencias que tienen bajo su custodia centros de cómputo y centros de cableado deben velar porque los niveles de temperatura y humedad relativa en estos sitios estén dentro de los límites requeridos por la infraestructura de cómputo allí instalada, para lo cual se deben usar sistemas de aire acondicionado según sea el caso.

- Las dependencias que tienen bajo su custodia centros de cómputo y/o centros de cableado deben solicitar mantenimientos preventivos y pruebas de funcionalidad del sistema de UPS y plantas eléctricas, de los sistemas de detección de incendios y del sistema de aire acondicionado.

8.1.2 Protección sobre amenazas externas y ambientales

Las dependencias que tienen en custodia centros de cómputo y/o centros de cableado deben monitorear las variables de temperatura y humedad de las áreas de procesamiento de datos.

El SENA debe designar y aplicar protección física para desastres como: fuego, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.

Las dependencias que tienen bajo su custodia centros de cómputo y/o centros de cableado deben velar por el ambiente adecuado para los activos informáticos como ventilación, iluminación, regulación de corriente, etc.

8.1.3 Trabajo en Áreas Seguras

El SENA debe mantener áreas seguras para la gestión, almacenamiento y procesamiento de información en la Entidad. Las áreas deben contar con:

- Protecciones físicas y ambientales, acordes con el valor y la necesidad de aseguramiento de los activos que se protegen.

- Definición de perímetros de seguridad.

- Controles de acceso físicos.

- Seguridad para protección de los equipos.

- Seguridad en el suministro eléctrico y cableado.

- Condiciones ambientales adecuadas de operación.

- Sistemas de contención, detección y extinción de incendios.

8.2 Equipos

8.2.3 Ubicación y Protección de los Equipos

- Los funcionarios, contratistas, instructores, aprendices y terceros no deben mover o reubicar los equipos de cómputo pertenecientes a la Entidad, instalar o desinstalar dispositivos, ni retirar marcas, logotipos ni hologramas de los mismos sin la autorización de la Oficina de Sistemas o quien haga sus veces.

- La Dirección Administrativa y Financiera debe resguardar los activos de información que se le asignan a los funcionarios, contratistas, instructores, aprendices y terceros mediante la firma del usuario como responsable de estos.

- Los funcionarios, contratistas, instructores, aprendices y terceros deben conservar los equipos de cómputo en la ubicación autorizada por la Oficina de Sistemas o quien haga sus veces.

- Los funcionarios, contratistas, instructores, aprendices y terceros deben utilizar los equipos de cómputo asignados para uso exclusivo de las funciones del cargo que desempeñan en la entidad.

- Los aprendices deben utilizar los equipos de cómputo destinados como herramientas de apoyo (salas de cómputo y laboratorios) a las labores académicas o de investigación, sin vulnerar las políticas establecidas por la Entidad y por las leyes vigentes del país.

- Los funcionarios, contratistas, instructores deben solicitar la capacitación necesaria para el

correcto manejo de las herramientas informáticas que requieren para realizar sus labores, a fin de evitar riesgos por mal uso y para aprovechar al máximo los recursos proporcionados por la entidad.

- Los funcionarios, contratistas, instructores, aprendices y terceros no deben consumir alimentos o ingerir líquidos mientras utilizan los equipos de cómputo.

- Los funcionarios, contratistas, instructores, aprendices y terceros deben informar a la Oficina de Sistemas o quien haga sus veces, cuando se requiera realizar cambios múltiples de los equipos de cómputo derivado de reubicación de lugares físicos de trabajo o cambios locativos, con varios días de anticipación y un plan detallado.

- Los funcionarios, contratistas, instructores, aprendices y terceros no deben abrir o destapar los equipos de cómputo de la Entidad. Solo el personal de la Oficina de Sistemas o quien haga sus veces, está autorizado para realizar esta labor.

8.2.1 Seguridad del Cableado

La Oficina de Sistemas o quien haga sus veces, debe mantener los cables de red de los centros de datos claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.

La Oficina de Sistemas o quien haga sus veces, y la Dirección Administrativa y Financiera deben contar con los planos que describan las conexiones del cableado.

La Oficina de Sistemas o quien haga sus veces, debe mantener el acceso a los centros de cableado solo para el personal autorizado.

8.2.2 Mantenimiento de Equipos

La Oficina de Sistemas o quien haga sus veces, es la responsable de llevar a cabo los servicios de mantenimiento y reparaciones al equipo informático, por medio de personal idóneo para la labor.

La Oficina de Sistemas o quien haga sus veces, es la única autorizada para realizar la labor descrita en el punto anterior.

Los funcionarios, contratistas, instructores, aprendices y terceros deben respaldar con copias de seguridad toda la información personal o clasificada que se encuentre en el equipo de cómputo asignado, previniendo así la pérdida involuntaria de la misma, derivada del proceso de reparación.

La Oficina de Sistemas o quien haga sus veces, debe realizar procedimientos de borrado seguro en los equipos que se dan de baja y los equipos que son asignados a usuarios diferentes por temas de rotación.

8.2.4 Equipos de usuarios desatendidos

Los funcionarios, contratistas, instructores, aprendices y terceros deben bloquear la sesión de sus equipos de cómputo cuando no se encuentren en su lugar de trabajo. Esto con el fin que la sesión del usuario no quede activa con los privilegios asignados.

Los aprendices deben cerrar sesión en los equipos de cómputo luego de terminar de usarlos para evitar el uso inadecuado de terceros.

8.2.5 Política de escritorio limpio y pantalla limpia

- Los funcionarios, contratistas, instructores, aprendices y terceros de la entidad deben conservar el escritorio del equipo, libre de información de uso interno o clasificada propia de la Entidad, que pueda ser alcanzada, copiada, alterada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

- La Oficina de Sistemas o quien haga sus veces, debe garantizar que los usuarios tengan la pantalla del equipo limpia o libre de archivos confidenciales por medio de mecanismos adecuados para este fin.

- La Oficina de Sistemas o quien haga sus veces, debe aplicar un protector estándar en todas las estaciones de trabajo y equipos portátiles de la entidad, de forma que se active luego de dos minutos sin uso.

- Los funcionarios, contratistas, instructores, aprendices y terceros deben guardar en un lugar seguro cualquier documento físico, medio magnético u óptico removible que contenga información clasificada o de uso interno.

- Los funcionarios, contratistas, instructores, aprendices y terceros no deben dejar en el escritorio físico documentos de uso clasificado sin custodia.

- La Oficina de Sistemas o quien haga sus veces, debe establecer las medidas de control necesarias que permitan comprobar el correcto cumplimiento de los puntos anteriores.

9 Seguridad de las Operaciones

9.1 Procedimientos operacionales y responsabilidades

- La Oficina de Sistemas o quien haga sus veces, debe realizar la documentación y actualización de los procedimientos relacionados con la operación y administración de los sistemas de información de la Entidad.

- La Oficina de Sistemas o quien haga sus veces, debe proporcionar a sus funcionarios manuales de configuración y operación de los servicios de red, bases de datos y sistemas de información que conforman las diferentes plataformas.

- La Oficina de Sistemas o quien haga sus veces, debe proveer los recursos necesarios para la implantación de controles que permitan la separación de ambientes de desarrollo, pruebas y producción, teniendo en cuenta consideraciones como:

- Controles para el intercambio de información entre los ambientes de desarrollo y producción.

- La inexistencia de compiladores, editores o fuentes en los ambientes de producción.

- Acceso diferente para cada uno de los ambientes.

9.1.1 Gestión de Cambios

- El SENA con el apoyo de la Oficina de Sistemas o quien haga sus veces, establecerá los

mecanismos para las solicitudes de cambios. De igual manera, coordinará y controlará los cambios realizados en los activos de información tecnológicos y los recursos informáticos.

- La Oficina de Sistemas o quien haga sus veces, debe garantizar que todo cambio realizado a un componente de la plataforma tecnológica, los cuales conlleve modificación de accesos, modificación o mantenimiento de software, actualización de versiones o modificación de parámetros, certifica y mantiene los niveles de seguridad existentes, no afecta la correcta operación de la misma ni de otros servicios.

- La Oficina de Sistemas o quien haga sus veces, debe garantizar que todo cambio realizado sobre la plataforma tecnológica de la entidad, quedará formalmente documentado desde su solicitud hasta su implementación.

- Los responsables de los activos de información tecnológicos y recursos informáticos (el Director General, Secretaría General, los Directores de área, Jefes de Oficina, Directores Regionales, Subdirectores de Centro y Coordinadores de Grupo) deben solicitar formalmente los requerimientos de nuevas funcionalidades, servicios o modificaciones sobre sus sistemas de información.

- La Oficina de Sistemas o quien haga sus veces, como Administradores de los activos de información tecnológicos y recursos informáticos, deben garantizar que las modificaciones o adiciones en las funcionalidades de los sistemas de información están soportadas por las solicitudes realizadas por los usuarios.

9.1.2 Gestión de capacidades

- La Oficina de Sistemas o quien haga sus veces, debe supervisar continuamente el uso de los recursos con el fin de realizar los pertinentes ajustes, mirar las proyecciones para las futuras necesidades de capacidad y asegurar el rendimiento del sistema requerido.

- La Oficina de Sistemas o quien haga sus veces, debe realizar estudios sobre las proyecciones de crecimiento de los recursos administrados de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica. Aspectos a considerar:

- Consumo de recursos de procesadores, memorias, discos.

- Servicios de impresión.

- Ancho de banda, internet y tráfico de las redes de datos.

9.1.3 Separación de Entornos de desarrollo, pruebas y producción

La Oficina de Sistemas o quien haga sus veces, debe separar los ambientes de desarrollo, pruebas y producción con el fin de reducir los riesgos de acceso no autorizado o cambios en el entorno operativo.

La Oficina de Sistemas o quien haga sus veces, debe garantizar los recursos necesarios que permitan la separación de los ambientes de desarrollo, pruebas y producción.

La Oficina de Sistemas o quien haga sus veces, debe garantizar la independencia de los usuarios que usan los ambientes de desarrollo, pruebas y producción.

9.2 Protección contra códigos maliciosos

9.2.1 Controles contra códigos maliciosos

- El SENA debe contar en cada uno de los equipos de la entidad con una licencia de antivirus y un agente instalado en cada una de ellos.

- Los funcionarios, contratistas, instructores, aprendices y terceros deben contar con un antivirus actualizado en sus dispositivos personales tales como: portátiles o celulares, si desean ingresar a la red de datos de la entidad.

- Los funcionarios, contratistas, instructores, aprendices y terceros deben verificar que la información y los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus instalado por la Oficina de Sistemas o quien haga sus veces, en los equipos de cómputo de la entidad.

- Los funcionarios, contratistas, instructores, aprendices y terceros deben verificar, mediante el uso del software de antivirus, que todo archivo, independiente de su procedencia, esté libre de virus antes de ser accedido.

- Ningún funcionario, contratista, instructor, aprendiz y terceros, debe descargar software desde sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de la Oficina de Sistemas o quien haga sus veces.

- Los funcionarios, contratistas, instructores, aprendices y terceros que sospechen de alguna infección por virus deben dejar de usar inmediatamente el equipo de cómputo y notificar a la Oficina de Sistemas o quien haga sus veces, para la revisión y eliminación del virus.

- Los funcionarios, contratistas, instructores, aprendices y terceros no deben realizar modificaciones o eliminar las configuraciones de seguridad en Antivirus, Outlook, office, navegadores u otros programas, para detectar y prevenir la propagación de virus.

- Los funcionarios, contratistas, instructores, aprendices y terceros no deben intentar eliminar los virus de los equipos, a menos que sea personal autorizado por la Oficina de Sistemas o quien haga sus veces, para garantizar la limpieza total de los equipos.

9.3 Copias de Respaldo

9.3.1 Respaldo de la información

El SENA, tiene el compromiso de la generación de copias de respaldo y almacenamiento de su información confidencial, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades.

Las áreas propietarias de la información, con el apoyo de la Oficina de Sistemas o quien haga sus veces, serán las encargadas de la generación de las copias de respaldo, se definirá la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.

Así mismo, se velará porque los medios magnéticos que contienen información de la entidad sean almacenados en una ubicación diferente a las instalaciones donde se encuentra disponible. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

9.3.1.1 Política para realizar copias de respaldo

- Para garantizar una correcta realización y seguridad de los backups (copias de respaldo) se deberán tener en cuenta los siguientes puntos por parte de la Oficina de Sistemas:

- Debe contar con un procedimiento de respaldo de los sistemas operativos y de la información de los usuarios, para poder realizar una reinstalación en caso de sufrir un percance.

- Debe determinar los medios y herramientas correctos para realizar los backups, teniendo en cuenta los espacios necesarios, tiempos de lectura escritura, tipo de backup a realizar, etc.

- Debe realizar el almacenamiento de los backups en lugares diferentes de donde reside la información principal. De este modo se evita la pérdida total si hay un desastre que afecte todas las instalaciones de la entidad.

- Debe verificar la integridad de los backups que se están almacenando, de acuerdo con el procedimiento de revisión periódica de estos, con el fin de asegurar que al momento de requerir restaurar alguno de ellos funcione como se espera.

- Debe contar con un procedimiento adecuado para garantizar la integridad física de los respaldos, en previsión de robo, destrucción o pérdida.

- Debe contar con un procedimiento previamente definido para borrar físicamente la información de los medios de almacenamiento, antes de desecharlos.

- Debe provisionar equipos de hardware con características similares a los utilizados para el proceso normal de la operación del SENA, en condiciones necesarias para entrar en funcionamiento en caso de desastres físicos.

- Debe garantizar la posterior recuperación sin pasos secundarios, que no generen impacto en la continuidad del negocio.

- Los directores, coordinadores, Jefes de Oficina, directores y subdirectores regionales, para el caso de la información confidencial, deben realizar el respaldo diario de las modificaciones efectuadas y guardar respaldos históricos semanalmente de dicha información mediante los mecanismos o herramientas proporcionadas por la Oficina de Sistemas o quien haga sus veces.

- Los directores, coordinadores, Jefes de Oficina, directores y subdirectores regionales para el caso de la información de uso interno deben respaldar con una frecuencia mínima de una semana y guardar los respaldos históricos mensualmente de la información mediante los mecanismos o herramientas proporcionadas por la Oficina de Sistemas o quien haga sus veces.

- Los directores, coordinadores, Jefes de Oficina, directores y subdirectores regionales para el caso de la información pública deben realizar el respaldo de ésta a criterio propio.

- Los directores, coordinadores, Jefes de Oficina, directores y subdirectores regionales como propietarios de los recursos tecnológicos y sistemas de información deben definir en conjunto con la Oficina de Sistemas o quien haga sus veces, las estrategias para la generación, retención y rotación de las copias de respaldo de los activos de información.

- Los directores, coordinadores, Jefes de Oficina, directores y subdirectores regionales deben identificar la información que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

9.3.1.2 Roles y Responsabilidades

La Oficina de Sistemas o quien haga sus veces, debe determinar los roles de usuario, según su responsabilidad y tareas asignadas dentro de la entidad, que intervienen dentro del proceso de backu ps:

- Administrador de backups: persona encargada de realizar los backups.

- Transportador: encargado de llevar los backups fuera de las instalaciones de la entidad.

- Operador: Encargado de probar backups cada cierto período de tiempo.

9.4 Registro y Seguimiento de Eventos de los sistemas de Información

- El SENA, realizará monitoreo permanente del uso que dan los funcionarios a los recursos de la plataforma tecnológica y los sistemas de información de la entidad. Además, velará por la custodia de los registros de auditoria cumpliendo con los periodos de retención establecidos para dichos registros.

- La Oficina de Sistemas o quien haga sus veces, en conjunto con los responsables de los servicios, definirán la realización de monitoreo de los registros de auditoría sobre los aplicativos donde se opera los procesos de la entidad.

- La Oficina de Sistemas o quien haga sus veces, debe determinar los eventos que generarán registros de auditoría en los recursos tecnológicos y los sistemas de información.

- La Oficina de Sistemas o quien haga sus veces, debe habilitar los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada, acorde con los eventos a auditar establecidos.

- La Oficina de Sistemas o quien haga sus veces, debe velar por la integridad y disponibilidad de los registros de auditoría generados en la plataforma tecnológica y los sistemas de información. Estos registros deben ser almacenados y sólo deben ser accedidos por personal autorizado.

9.5 Control de Software Operacional

9.5.1 Instalación de Software en sistemas operativos

- El SENA, a través de la Oficina de Sistemas o quien haga sus veces, designará responsables y establecerá procedimientos para controlar la instalación de software en los equipos informáticos, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software sea actualizado.

- La Oficina de Sistemas o quien haga sus veces, debe establecer responsabilidades y procedimientos para controlar la instalación del software en los equipos de cómputo.

- La Oficina de Sistemas o quien haga sus veces, debe asegurarse que tanto las aplicaciones desarrolladas in-house como las de terceros, realicen las respectivas pruebas antes de salir a producción.

- La Oficina de Sistemas o quien haga sus veces, debe asegurarse que el software instalado en la

plataforma tecnológica cuenta con soporte preciso en caso de ser necesario y con los proveedores según sea requerido.

- La Oficina de Sistemas o quien haga sus veces, debe conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software, así como monitorear dichas actualizaciones.

- La Oficina de Sistemas o quien haga sus veces, debe validar los riesgos que genera la migración hacia nuevas versiones del software.

- La Oficina de Sistemas o quien haga sus veces, debe asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software es actualizado.

- La Oficina de Sistemas o quien haga sus veces, debe establecer las restricciones y limitaciones para la instalación de software en los equipos de cómputo.

9.6 Gestión de Vulnerabilidades Técnicas

- El SENA, a través de la Dirección de planeación y Direccionamiento Corporativo, a través del Oficial de Seguridad de la información y en coordinación con la Oficina de Sistemas o quien haga sus veces, revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de la realización periódica de pruebas de vulnerabilidades (cada seis meses), con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas.

- La Oficina de Sistemas o quien haga sus veces, debe revisar cada tres meses o según se requiera, la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, con el fin de prevenir la exposición al riesgo de estos.

- La Oficina de Sistemas o quien haga sus veces, debe generar, ejecutar y monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica cada tres meses.

9.6.1 Restricciones sobre la instalación del software

La Oficina de Sistemas o quien haga sus veces, debe realizar la instalación de software en los computadores suministrados por la entidad, como función exclusiva de esta o a quienes ellos deleguen.

La Oficina de Sistemas o quien haga sus veces, debe autorizar el software adicional que se requiera instalar en equipos de cómputo específicos de la entidad.

La Oficina de Sistemas o quien haga sus veces, tendrá que mantener una lista actualizada del software autorizado para instalar en los computadores.

9.7 Consideraciones sobre auditorias de sistemas de información

9.7.1 Controles sobre auditorias de sistemas de información

- El SENA, a través de la Dirección de Planeación y la Oficina de Sistemas o quien haga sus veces, a su vez apoyada en los procedimientos de Auditoria Interna, verificará el cumplimiento

de los requisitos de las normas ISO aplicables, la normatividad legal vigente y los requisitos propios de la organización cada año o según sea necesario.

- La Oficina de Sistemas o quien haga sus veces, debe verificar que las auditorías concluyan la eficacia y eficiencia de los sistemas de información implementados en la institución.

- La Oficina de Sistemas o quien haga sus veces, debe planificar para reducir al mínimo las interrupciones de los procesos, de acuerdo a los requisitos de auditoría y las actividades relacionadas con la verificación de los sistemas operativos.

10 Seguridad de las Comunicaciones

10.1 Gestión de la seguridad de redes

- El SENA establecerá, a través de la Oficina de Sistemas o quien haga sus veces, 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 por 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.

- De igual manera, proporcionará el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información interna y confidencial de la institución.

- La Oficina de Sistemas o quien haga sus veces, debe adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red.

- La Oficina de Sistemas o quien haga sus veces, debe implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.

- La Oficina de Sistemas o quien haga sus veces, debe mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios y ubicación.

- La Oficina de Sistemas o quien haga sus veces, debe identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de nivel de servicios de red.

- La Oficina de Sistemas o quien haga sus veces, debe establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la institución, acogiendo buenas prácticas de configuración segura.

- La Oficina de Sistemas o quien haga sus veces, debe identificar, justificar y documentar los servicios, protocolos y puertos permitidos en la red de datos de la entidad e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.

- La Oficina de Sistemas o quien haga sus veces, debe instalar protección entre las redes internas y cualquier red externa, que esté fuera de la capacidad de control y administración de la entidad.

- La Oficina de Sistemas o quien haga sus veces, debe velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos.

10.2 Uso de la Mensajería Electrónica

- El Servicio Nacional de Aprendizaje - SENA, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre funcionarios y terceras partes,

proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones por este medio.

- La Oficina de Sistemas o quien haga sus veces, debe generar y divulgar un procedimiento para la administración de cuentas de correo electrónico; divulgar las normas para el uso de los servicios de correo electrónico; garantizar que la plataforma de correo tenga los procedimientos y controles necesarios que permitan detectar y proteger la integridad de la información que viaja a través de esta plataforma; asegurar que los mensajes electrónicos están protegidos contra código malicioso y pudiera ser transmitido a través de estos; generar campañas de concientización a todos sus usuarios (directores, coordinadores, Jefes de Oficina, directores y subdirectores regionales, contratistas, aprendices, etc.), respecto a las precauciones que deben adoptar en el intercambio de información confidencial y de uso interno por medio del correo electrónico.

- Los directores, Secretaría General, Jefes de Oficina, directores y subdirectores regionales, coordinadores, contratistas y aprendices, deben saber que la cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún funcionario, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.

- Los directores, Secretaría General, Jefes de Oficina, directores y subdirectores regionales, coordinadores, contratistas y aprendices, deben designar responsables para la administración de las cuentas institucionales, donde estas personas responderán por las mismas.

- Los directores, Secretaría General, Jefes de Oficina, directores y subdirectores regionales, coordinadores, contratistas y aprendices, deben utilizar el correo electrónico para envío de mensajes e información relacionada con el desarrollo de las labores y funciones asignadas a cada usuario.

- El personal del SENA no debe utilizar el correo electrónico institucional para actividades personales de ninguna índole, entre otras, el envío de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los miembros de la entidad.

- Los directores, Secretaría General, Jefes de Oficina, directores y subdirectores regionales, coordinadores, contratistas y aprendices, deben mantener solamente los mensajes relacionados con el desarrollo de sus funciones, puesto que los mensajes e información contenida en los buzones de correo son propiedad de la entidad.

- Los directores, Secretaría General, Jefes de Oficina, directores y subdirectores regionales, coordinadores, contratistas, aprendices y terceros, no deben enviar archivos que contengan extensiones ejecutables con contenido malicioso, por ningún motivo.

- Los directores, Secretaría General, Jefes de Oficina, directores y subdirectores regionales, coordinadores, contratistas, aprendices y terceros deben respetar el estándar de formato e imagen corporativa definidos por la entidad para los mensajes electrónicos y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

10.3 Uso adecuado del servicio de Internet

- El SENA, consciente de la importancia de internet como una herramienta para el desempeño de las labores diarias, proporcionará los recursos necesarios para asegurar su disponibilidad a los

usuarios que así lo requieran para el desarrollo de sus actividades en la entidad.

- La Oficina de Sistemas o quien haga sus veces, debe: Proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de internet, bajo las restricciones de los perfiles de acceso establecidos; implementar mecanismos que permitan la continuidad o restablecimiento del servicio de internet en caso de contingencia interna; monitorear continuamente el canal o canales del servicio de internet, en cuanto a carga y tráfico; establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de internet y evitar el acceso a sitios catalogados como restringidos; generar registros de la navegación y los accesos de los usuarios a internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de internet.

- La Oficina de Sistemas o quien haga sus veces, en acompañamiento con Secretaria General y la Direccion de Planeacion deben generar campañas para concientizar a todo el personal del SENA y terceros, respecto a las precauciones que deben tener en cuenta cuando utilicen el servicio de internet.

- La comunidad SENA y terceros deben hacer uso del servicio de internet que provee la entidad para las actividades que guarden relación con su labor dentro de la misma; abstenerse de descargar software no autorizado desde internet, así como su instalación en las estaciones de trabajo asignados para el desempeño de sus labores, a menos que sean autorizados por la Oficina de Sistemas o quien haga sus veces.

- Todo el personal del SENA y terceros no deben acceder a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y cualquier otra página que vaya en contra de la ética y la moral, las leyes vigentes del país o las políticas establecidas en este documento, a menos que la labor que tiene en la entidad, así lo demande.

- Todo el personal del SENA y terceros no deben utilizar el servicio de internet para el acceso y uso de servicios interactivos o mensajería instantánea como Facebook y otros similares, con el fin de intercambiar información confidencial o de uso interno de la entidad o para actividades que no corresponden con el desempeño de las funciones asignadas.

- Todo el personal del SENA y terceros no deben descargar, usar, intercambiar o instalar juegos, música, películas, información que de alguna manera atenten contra la propiedad intelectual de sus autores.

- Todo el personal del SENA y terceros no deben ejecutar archivos o herramientas que atenten contra la integridad, disponibilidad o confidencialidad de la infraestructura tecnológica de la entidad.

- Todo el personal del SENA y terceros deben asegurarse de que la información audiovisual (videos e imágenes) descargada y utilizada para las labores diarias no atenten contra la propiedad intelectual de sus autores.

- Todo el personal del SENA y terceros no deben intercambiar de ninguna forma, información confidencial para la entidad sin la debida autorización.

10.4 Transferencia de Información

El SENA, asegurará la protección de la información en el momento de ser transferida o intercambiada con otras entidades y establecerá los procedimientos y controles necesarios para el intercambio de información; así mismo, se establecerán Acuerdos de Confidencialidad o de Intercambio de Información con las terceras partes con quienes se realice dicho intercambio. La entidad velará por el uso de tecnologías informáticas y de telecomunicaciones para llevar a cabo el intercambio de información; sin embargo, establecerá directrices para el intercambio de información en medio físico.

10.4.1 Políticas y procedimientos de transferencia o transmisión de información

- La Dirección Jurídica, en acompañamiento con la Dirección de Planeación y a Oficina de Sistemas o quien haga sus veces, debe definir los modelos de Convenios o Contratos de Transferencia o Transmisión de datos, así como las cláusulas de Confidencialidad de información entre la institución y terceras partes incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos.

- Entre los aspectos a considerar se debe incluir:

- La prohibición de divulgar la información entregada por parte de la entidad a los terceros con quienes se establecen estos acuerdos.

- La destrucción de dicha información una vez cumpla su cometido.

- La Dirección Jurídica debe establecer en los contratos que se constituyan con terceras partes, los acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la divulgación no autorizada de información de la entidad que les ha sido entregada.

- La Oficina de Sistemas o quien haga sus veces, debe velar porque el intercambio de información con entidades externas se realice en cumplimiento de este Manual de Políticas de Seguridad, los Acuerdos de Intercambio de Información y el procedimiento definido para dicho intercambio de información.

- Todo el personal del SENA y terceros deben utilizar únicamente los mecanismos y herramientas proporcionadas por la Oficina de Sistemas o quien haga sus veces para el envío o recepción de información confidencial para la entidad.

- Queda prohibido que el personal del SENA y terceros revelen o intercambien información confidencial de la entidad por cualquier medio, sin contar con la debida autorización y documento "convenio" que la garantice y del titular de la información cuando haya lugar a ello.

11 Adquisición, Desarrollo y Mantenimiento de Sistemas

11.1 Requisitos de seguridad de los sistemas de información

- El SENA, garantizará que el software adquirido y desarrollado tanto al interior de la entidad como por terceras partes, cumplirá con los requisitos de seguridad y calidad establecidos por la entidad. Las áreas propietarias de sistemas de información y la Oficina de Sistemas o quien haga sus veces, 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.

- La Oficina de Sistemas o quien haga sus veces debe aprobar la compra de los aplicativos o el software en concordancia con la política de adquisición de bienes de la entidad.

- La Oficina de Sistemas o quien haga sus veces debe establecer metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro.

- Las áreas propietarias de los sistemas de información, en acompañamiento con La Oficina de Sistemas o quien haga sus veces, deben establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando los requerimientos de seguridad de la información.

- Las áreas propietarias de los sistemas de información deben definir qué información confidencial puede ser eliminada de sus sistemas y solicitar que estos soporten la eliminación de dicha información, como es el caso de los datos personales o financieros, cuando estos ya no son requeridos.

- La Oficina de Sistemas o quien haga sus veces debe liderar la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones, entre otros.

- Los desarrolladores deben documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se quiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles deseados.

- Los desarrolladores deben certificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas y reconocidas en el mercado.

- Los desarrolladores deben deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.

- Los desarrolladores deben cerrar las sesiones activas de las aplicaciones luego que pasen tres minutos sin actividad, terminándolas una vez se cumpla este tiempo.

- Los desarrolladores deben asegurar que no se permitan conexiones recurrentes a los sistemas de información con el mismo usuario.

- Los desarrolladores deben utilizar usar los protocolos sugeridos por La Oficina de Sistemas o quien haga sus veces en los aplicativos desarrollados.

- Los desarrolladores deben realizar la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros y utilizando mecanismos o herramientas de cifrado.

- Personal del SENA y terceros que desarrollen un sistema de información deben proporcionar los respectivos manuales, como son:

- Manual del usuario que describa los procedimientos de operación.
- Manual técnico que describa su estructura interna, programas, catálogos y archivos.

11.2 Seguridad en los procesos de desarrollo y de soporte

11.2.1 Política de desarrollo seguro

- El SENA velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por la institución.

- La Oficina de Sistemas o quien haga sus veces en conjunto con los propietarios de los aplicativos deben realizar las pruebas necesarias para asegurar que los sistemas de información desarrollados cumplen con los requerimientos de seguridad establecidos antes del paso a producción.

- La Oficina de Sistemas o quien haga sus veces en conjunto con los propietarios de los aplicativos deben realizar las pruebas de los sistemas de información utilizando metodologías establecidas para este fin, documentado las pruebas realizadas y aprobando los pasos a producción.

- La Oficina de Sistemas o quien haga sus veces en conjunto con los propietarios de los aplicativos deben realizar las pruebas por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.

- La Oficina de Sistemas o quien haga sus veces en conjunto con los propietarios de los aplicativos deben aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos y de cambios o nuevas funcionalidades.

- La Oficina de Sistemas o quien haga sus veces debe implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.

- La Oficina de Sistemas o quien haga sus veces debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información.

- La Oficina de Sistemas o quien haga sus veces debe asegurase que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

- La Oficina de Sistemas o quien haga sus veces debe generar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.

- La Oficina de Sistemas o quien haga sus veces debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.

- La Oficina de Sistemas o quien haga sus veces debe incluir dentro del procedimiento y los controles de gestión de cambios el manejo de los cambios en el software aplicativo y los sistemas de información de la institución.

- Los desarrolladores de los sistemas de información deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.

- Los desarrolladores deben proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el aplicativo; dicho soporte debe contemplar tiempos de respuesta aceptables.

- Los desarrolladores deben construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.

- Los desarrolladores deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como:

- Tipos de datos
- Rangos válidos
- Longitud

- Listas de caracteres aceptados
- Caracteres considerados peligrosos
- Caracteres de alteración de rutas.

- Los desarrolladores deben suministrar opciones de desconexión o cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.

- Los desarrolladores deben asegurar el manejo de operaciones sensibles o críticas en los aplicativos desarrollados permitiendo el uso de dispositivos adicionales como parámetros adicionales de verificación.

- Los desarrolladores deben asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos.

- Los desarrolladores deben garantizar que no se divulgue información confidencial en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.

- Los desarrolladores deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.

- Los desarrolladores deben prevenir la revelación de la estructura de directorios de los sistemas de información construidos.

- Los desarrolladores deben remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.

- Los desarrolladores deben evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.

- Los desarrolladores deben certificar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.

- Los desarrolladores deben generar los controles necesarios para la transferencia de archivos, como:

-- Exigir autenticación

-- Vigilar los tipos de archivos a transmitir

-- Almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos.

-- Eliminar privilegios de ejecución a los archivos transferidos.

-- Asegurar que dichos archivos sólo tengan privilegios de lectura.

- Los desarrolladores deben proteger el código fuente de las aplicaciones construidas, de tal forma de que no pueda ser descargado ni modificado por los usuarios.

- Los desarrolladores deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

11.3 Datos de prueba

11.3.1 Protección de datos de prueba

- La Oficina de Sistemas o quien haga sus veces, protegerá los datos de prueba que se entregarán a los desarrolladores, asegurando que no revelan información confidencial de los ambientes de producción.

- La Oficina de Sistemas o quien haga sus veces, debe certificar que la información entregada a los desarrolladores para realizar sus pruebas no revelará información confidencial de los ambientes de producción.

- La Oficina de Sistemas o quien haga sus veces debe eliminar la información de los ambientes de pruebas, una vez estas han concluido.

12 Relaciones con los Proveedores

El SENA, 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.

Dada la cantidad de procesos de intercambio de información en los que participa la entidad (tanto interno como externo) y buscando mantener la confidencialidad, disponibilidad e integridad de la misma, se señalan los siguientes lineamientos:

- En todos los Acuerdos con terceras partes, que implique un intercambio, uso o procesamiento de información de la Entidad, se deben realizar Acuerdos de Confidencialidad sobre el manejo de la información.

- Los Acuerdos de confidencialidad de la información deben hacer parte integral de los contratos o documentos que legalicen la relación del negocio.

- Dentro de los acuerdos que suscriba el SENA, se deberá definir claramente el tipo de información que se va a intercambiar por las partes.

- Las dependencias que suscriban acuerdos, contratos, y/o convenios se asegurarán de la divulgación de las políticas, normas y procedimientos de seguridad de la información.

- las partes involucradas deben aceptar que toda la información compartida es confidencial (exceptuando los datos públicos) y por tanto deciden establecer los términos que rigen su uso y la protección de dicha información.

- Se deberá realizar de manera previa entre las partes un análisis del contexto de la información a compartir, esto es identificar el nivel de riesgo de la información).

- Se beberá dar estricto cumplimiento a los deberes contemplados en la ley 1266 de 2008, en los artículos 17 y 18 de la Ley 1581 de 2012; la ley 1437 de 2011, ley 1712 de 2014 y sus decretos reglamentarios.

- Las partes guardaran confidencialidad respecto del tratamiento de los datos personales privados y sensibles contenidos en el intercambio de información de acuerdo con lo exigido por la ley 1581 de 2012 y su decreto reglamentario.

- No deben utilizar y/o emplear la información que reciban de la contraparte, para fines distintos a los señalados.

- La Dirección, oficina y/o dependencia que suscriba cualquier tipo de acuerdo deberá determinar los responsables dentro de sus dependencias, los que además deberán participarán en el proceso de intercambio de información en ambas entidades.

- Realizar de manera previa a la suscripción del convenio, contrato y/o acuerdo la clasificación de la información que se entrega y se recibe.

Las Direcciones, oficinas y/o dependencias que como mínimo debe estar involucradas de manera previa a la suscripción del acuerdo, convenio u contrato son:

- Dirección, oficina o dependencia que suscribirá el acuerdo.

- Oficial de Seguridad de la Información CISO de la Dirección de Planeación y Direccionamiento Corporativo. (como apoyo transversal y de consulta)

- Oficina de Sistemas. (TI).

Para la celebración de un acuerdo, convenio u contrato se requerirá la suscripción de un anexo técnico, donde se establecerá un protocolo de intercambio de la información y se fijarán las condiciones técnicas y controles de seguridad que se utilizarán para proteger la información, de la siguiente manera:

- Una vez clasificada la información, en coordinación con el oficial de seguridad de la información (CISO) de la Dirección de Planeación y Direccionamiento Corporativo y en coordinación con La Oficina de Sistemas o quien haga sus veces, se debe establecer entre las partes el tipo de Infraestructura que soportará el convenio.

- De manera coordinada la dependencia que suscribirá el acuerdo, convenio u contrato y La

Oficina de Sistemas o quien haga sus veces se diseñará el mapa lógico del proceso. (donde se evidencie la infraestructura, servicios y áreas involucradas), así mismo; se establecerá de manera conjunta entre las partes del acuerdo, convenio u contrato la infraestructura de seguridad requerida que soportara el proceso, (VPN, ftp, cifrado de información, certificado digital, etc.).

- Se deberán definir los responsables técnicos, es decir quienes custodiaran la infraestructura y la seguridad del proceso de intercambio.

- Determinar los responsables funcionales, quienes extraerán la información requerida dentro de las bases de datos de la entidad.

12.1 Política de seguridad de la información para las relaciones con los proveedores

- Cuando se celebre un acuerdo, convenio u contrato, los cuales pueden incluir intercambio de información del SENA, el área o dirección que lo celebre en coordinación con la Oficina de Sistemas o quien haga sus veces, debe establecer las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la Entidad.

- La Oficina de Sistemas o quien haga sus veces y el grupo de Convenios deben generar una guía base para los Acuerdos de Niveles de Servicio y requisitos de Seguridad informática, con los que deben cumplir los proveedores de servicios; dicha guía debe ser divulgado a todas las áreas que adquieran o supervisen recursos o servicios tecnológicos.

- La Oficina de Sistemas y el grupo de convenios deben elaborar modelos de Acuerdos de Confidencialidad y Acuerdos de Intercambio de Información con terceras partes. De dichos acuerdos deberán derivarse una responsabilidad tanto civil como penal para la tercera parte contratada.

- La Oficina de Sistemas debera establecer las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la entidad.

- La Oficina de Sistemas deberá mitigar los riesgos relacionados con terceras partes que tengan acceso a los sistemas de información y la plataforma tecnológica.

12.2 Gestión de la Prestación de Servicios de Proveedores

El SENA velará por mantener los niveles acordados de seguridad de la información y de prestación de los servicios de los proveedores, en concordancia con los acuerdos establecidos con ellos. Así mismo, velará por la adecuada gestión de cambios en la prestación de servicios de dichos proveedores.

La Oficina de Sistemas o quien haga sus veces y Recursos Informáticos debe verificar el momento pertinente para que el proveedor realice la conexión, apegándose a las condiciones de conexión de los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la institución.

13 Gestión de Incidentes de Seguridad de la Información

13.1 Gestión de incidentes y mejoras en la seguridad de la información

- La Dirección de Planeación y Direccionamiento Corporativo en coordinación con la Oficina de Sistemas o quien haga sus veces, presentará un reporte de incidentes relacionado con la

seguridad de la información al comité directivo.

- La Dirección de Planeación y Direccionamiento Corporativo en coordinación con la Oficina de Sistemas, realizarán la gestión del tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.

- De igual manera, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.

- Las directivas de la entidad serán la única autorizada para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

13.1.1 Responsabilidades y procedimientos

- El Director General, Secretaría General, los Directores de área, Jefes de Oficina, Directores Regionales, Subdirectores de Centro y Coordinadores de Grupo como propietarios de los activos de información deben reportar a la Direccion de Planeación y a la Oficina de Sistemas o quien haga sus veces los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.

- La Direccion de Planeacion debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.

- La Direccion de Planeacion en cooperación con la Oficina de Sistemas o quien haga sus veces debe evaluar todos los incidentes de seguridad de acuerdo a sus circunstancias particulares y escalar aquellos en los que se considere pertinente.

- La Direccion de Planeacion y la Oficina de Sistemas o quien haga sus veces deben designar personal calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su ocurrencia nuevamente.

- La Direccion de Planeacion y la Oficina de Sistemas o quien haga sus veces deben crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.

- Todo el personal del SENA y terceros deben reportar cualquier evento o incidente relacionado con la seguridad de la información y los recursos tecnológicos con la mayor prontitud posible.

- Todo el personal del SENA y terceros deben informar, en caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno o confidencial, a la Direccion de Planeacion y la Oficina de Sistemas o quien haga sus veces, para que se registre y se le dé el trámite necesario.

14 Aspectos de Seguridad para la Gestión de Continuidad de Negocios

14.1 Continuidad de Seguridad de la Información

- El SENA, debe garantizar que los planes de continuidad de negocios se ejecuten de forma segura sin exponer la información de la entidad.

- El SENA, debe asegurar la continuidad del componente de seguridad de la información ante la ocurrencia de eventos no previstos y debe contar y asegurar la implementación de un Plan de Recuperación de Desastres que asegure la continuidad de las operaciones tecnológicas de sus procesos críticos.

- Para el SENA su recurso más importante es el Recurso Humano y por lo tanto será su prioridad y objetivo principal protegerlo adecuadamente en cualquier situación.

- El SENA, debe tener un plan de contingencias que le permita evaluar los niveles de recuperación que requiere la entidad, así como los requerimientos de seguridad, funciones, responsabilidades relacionados con el plan.

- El SENA debe establecer un plan de pruebas periódico del plan de Contingencia de la Plataforma Tecnológica.

15 Cumplimiento

15.1 Cumplimiento de requisitos legales y contractuales

El SENA 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.

15.1.1 Identificación de la legislación aplicable y de los requisitos contractuales

- La dirección Jurídica, la dirección de planeación y La Oficina de Sistemas o quien haga sus veces deben identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la institución y relacionados con seguridad de la información.

- La Oficina de Sistemas o quien haga sus veces debe certificar que todo el software que se ejecuta en la institución esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.

- Nadie del personal del SENA y terceros está autorizado a instalar software en sus estaciones de trabajo suministrados para el desarrollo de sus actividades sin la autorización de La Oficina de Sistemas o quien haga sus veces, a menos que su labor así lo requiera, acogiéndose al buen uso y licenciamiento del software que se está utilizando.

- Todo el personal de SENA y terceros deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software sin la autorización del propietario de los derechos de autor y su reproducción no autorizada es una violación de ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada.

15.1.2 Privacidad y protección de información de datos personales

- El SENA, en el diseño e implementación de la política de seguridad de la información y Protección de Datos Personales, velará por que los encargados del Tratamiento den cabal cumplimiento a las disposiciones consagradas en la Constitución Política de Colombia, contemplados en los artículos 15 y 20, la Ley 1286 de 2008, la Ley Estatutaria 1581 de 2012 el Decreto 1377 de 2013 que reglamenta parcialmente la Ley 1581 de 2012, "por la cual se dictan disposiciones generales para la protección de datos personales"., la entidad velará por la protección de los datos personales de sus funcionarios, contratistas, aprendices, proveedores, graduados y demás terceros de los cuales reciba y administre información. En su elaboración, desarrollo y aplicación se tendrán en cuenta entre otros, los siguientes aspectos.

- Se establecerán los términos, condiciones y finalidades para las cuales la entidad como responsable de los datos personales obtenidos en sus distintos canales, tratará la información de todas las personas que, en algún momento, por razones de la actividad que desarrolla la entidad, hayan suministrado datos personales.

- Así mismo, buscará proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información que la entidad conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias del negocio y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

- Las áreas que procesan datos personales de aprendices, instructores, funcionarios, contratistas y terceros deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la entidad.

- Las áreas que procesan datos personales de aprendices, instructores, funcionarios, contratistas y terceros deben asegurar que solo aquellas personas que tengan una relación laboral legítima puedan tener acceso a dichos datos.

- Las áreas que procesan datos personales de aprendices, instructores, funcionarios, contratistas y terceros deben acoger las directrices técnicas y procedimientos establecidos para enviar mensajes por correo electrónico a dichos usuarios.

- La Oficina de Sistemas o quien haga sus veces debe establecer los controles para el tratamiento y protección de los datos personales de los aprendices, instructores, funcionarios, contratistas y terceros de los cuales reciba y administre información almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación, sin la autorización requerida.

- Los funcionarios, contratistas, instructores, aprendices y terceros deben guardar la discreción correspondiente o la reserva absoluta con respecto a la información de la información o de sus funcionarios de la cual tengan conocimiento en el ejercicio de sus funciones.

- Los funcionarios, contratistas, instructores, aprendices y terceros deben verificar la identidad de todas aquellas personas a quienes se les entrega información por teléfono, por correo electrónico o certificado, entre otros.

- Los usuarios que se registren en los sistemas de información de la entidad, deben aceptar el suministro de datos personales que pueda hacer la entidad a los terceros delegados para el tratamiento de datos personales, a entidades judiciales y demás entes del Estado que, en ejercicio de sus funciones, solicitan esta información.

15.2 Revisiones de seguridad de la información

15.2.1 Cumplimiento con las políticas de seguridad de la Información

La Dirección de Planeación en cooperación con la Oficina de Sistemas o quien haga sus veces, velaran por el cumplimiento de normas y políticas de seguridad y controles, que garanticen acciones preventivas y correctivas para salvaguardar la información digital y física, los equipos de cómputo e instalaciones de cómputo, así como de las bases de datos de información automatizada en general.

15.2.1.1 Cláusulas de Cumplimiento

- La Dirección de Planeación debe gestionar la verificación del cumplimiento del Manual de Políticas de Seguridad de la Información.

- La Oficina de Sistemas o quien haga sus veces puede implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo. El mal uso de los recursos informáticos que sea detectado será reportado.

- Los directores, coordinadores, Jefes de Oficina, directores y subdirectores regionales como dueños de los procesos establecidos en la entidad deben apoyar las revisiones del cumplimiento de las políticas de seguridad de la información que les competa y cualquier otro requerimiento de seguridad.

15.2.1.2 Violaciones de seguridad Informática

- Todo el personal del SENA y terceros no deben hacer uso de herramientas de hardware o software para violar los controles de seguridad de la Información, a menos que se autorice por La Oficina de Sistemas o quien haga sus veces.

- Nadie del personal del SENA y terceros debe probar o intentar probar fallas de la Seguridad Informática conocidas, a menos que estas pruebas sean controladas y aprobadas por La Oficina de Sistemas o quien haga sus veces.

- Nadie del personal del SENA y terceros debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a los equipos de cómputo, redes o información de la entidad.

- Nadie del personal del SENA y terceros debe hacer uso de los recursos asignados para actividades no relacionadas con el propósito de la entidad o bien con la extralimitación en su uso.

- Nadie del personal del SENA y terceros debe traer equipos o ejecutar aplicaciones que no estén directamente especificados como parte del software, hardware o de los estándares de los recursos informáticos propios de la entidad.

- Nadie del personal del SENA y terceros debe introducir en los Sistemas de Información o la Red de la entidad contenidos obscenos, amenazadores, inmorales u ofensivos.

- Nadie del personal del SENA y terceros debe introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres

que causen o sean susceptibles de causar cualquier tipo de alteración o daño a la información o los recursos informáticos.

- Nadie del personal del SENA y terceros debe intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.

- Nadie del personal del SENA y terceros debe albergar datos de carácter personal en carpetas diferentes a la asignada para este fin, en las estaciones de trabajo.

- Cualquier archivo introducido en la red corporativa o en el puesto de trabajo del usuario a través de soportes automatizados, internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual y control de virus.

16 Política de Privacidad y Protección de datos personales

16.1.1 Marco Legal

Constitución Política de Colombia	Artículos 2 fines esenciales del estado, 15 del Habeas Data, 20 y 74 sobre acceso a la Información
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
Ley Estatutaria 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones
Decreto Único Reglamentario 1081 de 2015 del Sector Presidencia de la República, compiló el Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Sentencias de la Corte Constitucional	C-1011 de 2008 mediante la cual se estudia la exequibilidad de la Ley Estatutaria 1266 de 2008. C-748 de 2011 mediante la cual se estudia la exequibilidad de la Ley Estatutaria 1581 de 20

16.2 Principios Rectores

Acorde con la aplicación de la ley 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales y las normas que la complementan, modifican o adicionan, se aplicarán de manera armónica e integral los siguientes principios rectores:

- Principio de Legalidad: La recolección, uso y tratamiento de datos personales se fundamentará en lo establecido por la Ley y las demás disposiciones que la desarrollen.

- Principio de Finalidad: La recolección, uso y tratamiento de datos personales obedecerán a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual será informada al titular de los

datos.

- Principio de libertad: La recolección, uso y tratamiento de datos personales sólo puede ejercerse con el consentimiento previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

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

- Principio de transparencia: En la recolección, uso y tratamiento de datos personales debe garantizarse el derecho del titular a obtener del responsable del tratamiento o del encargado de tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

- Principio de acceso y circulación restringida: La recolección, uso y tratamiento de datos sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la Ley y demás normas que la desarrollan. Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a la ley.

- Principio de seguridad: La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- Principio de confidencialidad: Todas las personas que intervengan en la recolección, uso y tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, incluso luego de finalizada su relación con alguna de las labores que comprende el tratamiento.

- Principio de celeridad: Este principio busca la agilidad en el trámite y la gestión administrativa.

16.3 Categorías Especiales de Datos

16.3.1 Datos Sensibles

Datos sensibles son 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.

- El SENA garantizará 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 o quien haga

sus veces, 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.

- Todas las áreas que procesan datos personales de beneficiarios, servidores públicos, aprendices, proveedores y partes interesadas, deben obtener la autorización, para el tratamiento de estos datos, con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir, dichos datos personales en el desarrollo de las funciones propias de la entidad.

- Todas las áreas que procesan datos personales de beneficiarios, servidores públicos, aprendices, proveedores y partes interesadas, deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima, de acuerdo a sus funciones y responsabilidades, puedan tener acceso a dichos datos.

- Todas las áreas que procesan datos personales de beneficiarios, servidores públicos, aprendices, proveedores y partes interesadas, deben establecer condiciones contractuales y de seguridad, a las entidades vinculadas, para el tratamiento de dichos datos personales.

- Todas las áreas que procesan datos personales de beneficiarios, servidores públicos, aprendices, proveedores y partes interesadas, deben cumplir con las directrices técnicas establecidas, para enviar datos personales a los propietarios, mediante el correo electrónico y/o mensajes de texto.

- La Oficina de Sistemas o quien haga sus veces de establecer los controles respectivos, para el tratamiento y protección de los datos personales de los beneficiarios, servidores públicos, aprendices, proveedores y partes interesadas, contenidos en los sistemas de información o repositorios, bajo su propiedad.

- Todo el personal del SENA y los contratistas, es decir, todos los servidores públicos, aprendices, proveedores y partes interesadas, deben:

-- Guardar la discreción correspondiente, o la reserva absoluta, con respecto a la información de la entidad o del personal, el cual, teniendo en cuenta sus funciones, tiene acceso a los datos personales almacenados en la plataforma tecnológica del SENA.

-- Todo el personal del SENA y terceros, deben verificar la identidad de todas aquellas personas, a quienes se les entrega datos personales por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.

-- Todo el personal del SENA y terceros deben asumir la responsabilidad individual, sobre las claves de acceso a sistemas de información, repositorios y recursos informáticos de la entidad, que almacenen datos personales.

-- Todo el personal del SENA y terceros deben aceptar el suministro de datos personales, que pueda hacer la entidad, a terceros, para el tratamiento de datos personales, a entidades judiciales y demás entes del Estado que, en ejercicio de sus funciones, solicitan esta información; de igual manera, deben aceptar que pueden ser objeto de procesos de auditoria interna o externa.

16.3.2 Tratamiento de datos sensibles

Se prohíbe el tratamiento de datos sensibles, excepto cuando:

- El titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.

- El tratamiento sea necesario para salvaguardar el interés vital del titular y éste se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.

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

- El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

- El tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los titulares.

16.4 Derechos de los niños, niñas y adolescentes

En la recolección, uso y tratamiento de los datos personales, 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 de sus entidades proveer el 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.

16.5 Excepciones de Acceso a la Información

El acceso a datos personales corresponde a una excepción de acceso a la información pública nacional, enmarcadas en el título III de la Ley 1712 de 2014.

16.6 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 el título "Tratamiento de la información y finalidad de los datos" del presente documento, la ley reglamentaria y la normatividad vigente.

16.7 Tratamiento de la información y finalidad de los datos

La autorización previa del titular de los datos personales, salvo en los casos autorizados por la ley, le permitirá al Servicio Nacional de Aprendizaje - SENA, dar el siguiente tratamiento a la información:

- Para los fines administrativos propios de la entidad.

- Caracterizar ciudadanos y grupos de interés y adelantar estrategias de mejoramiento en la

prestación del servicio.

- Dar tratamiento y respuesta a las peticiones, quejas, reclamos, sugerencias y/o felicitaciones presentados a la entidad.

- Alimentar el Sistema de Información y Gestión de Empleo Público - SIGEP.

- Conocer y consultar la información del titular del dato que repose en bases de datos de entidades públicas o privadas.

- Adelantar encuestas de satisfacción de usuarios.

- Envío de información de interés general.

- Recopilar información de ciudadanos asistentes a capacitaciones desarrolladas por la entidad.

- Medición de calidad e impacto de los servicios en la población objeto de atención.

- Conformar y mantener actualizada la base de datos del SENA.

La información y datos personales suministrados por el titular de los mismos, podrán ser utilizados por el SENA para el desarrollo de las funciones propias de la entidad.

Cualquier otro tipo de finalidad que se pretenda dar a los datos personales, salvo los casos autorizados por la Ley, deberá ser informado previamente en el aviso de privacidad y en la respectiva autorización otorgada por el titular del dato.

Todos los datos deberán estar almacenados en un servidor del SENA en Colombia, lugar donde deberán estar n custodiados con mecanismos avanzados de seguridad informática, con el objetivo de evitar el acceso no autorizado por parte de terceros a su información.

16.8 Derechos de los titulares de los datos personales

- El SENA, garantiza al titular de datos personales, el pleno ejercicio de los siguientes derechos:

- Conocer, actualizar y rectificar sus datos personales. Este derecho se podrá ejercer también, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.

- Solicitar prueba de la autorización otorgada al SENA para el tratamiento de sus datos personales.

- Ser informado del uso y tratamiento dado a sus datos personales, previa solicitud elevada a través de los canales de servicio.

- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la ley y las demás normas que la modifiquen, adicionen o complementen.

- Revocar la autorización y/o solicitar la supresión de uno a más datos cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el tratamiento de los datos se ha incurrido en conductas contrarias a la ley y a la Constitución.

- Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

16.9 Deberes del Servicio Nacional de Aprendizaje SENA como Responsable del Tratamiento de los Datos Personales

El Servicio Nacional de Aprendizaje SENA, actuando en calidad de responsable del tratamiento de datos personales, deberá:

- Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

- Solicitar y conservar copia de la respectiva autorización otorgada por el titular, para el uso y tratamiento de los datos personales.

- Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten, en virtud de la autorización otorgada.

- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- Garantizar que la información que se suministre al encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.

- Actualizar la información, comunicando de forma oportuna al encargado del tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a éste, se mantenga actualizada.

- Rectificar la información cuando sea incorrecta y comunicar lo pertinente al encargado del tratamiento.

- Suministrar al encargado del tratamiento, según el caso, únicamente datos cuyo tratamiento esté previamente autorizado.

- Exigir al encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular.

- Tramitar las consultas y reclamos formulados.

- Abstenerse de circular información que esté siendo controvertida por el titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.

- Registrar en la base de datos respectiva, la leyenda "reclamo en trámite" en la forma en que se regula en la presente ley.

- Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.

- Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.

- Informar a solicitud del titular sobre el uso dado a sus datos.

- Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.

- Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y

Comercio.

16.10 Aviso de Privacidad

- Cuando no sea posible poner a disposición del titular la Política de Tratamiento de la Información, el Servicio Nacional de Aprendizaje SENA, informará por medio de un Aviso de Privacidad, sobre la existencia de tales políticas.

- El Aviso de Privacidad se encuentra publicado en la página web de la entidad www.sena.edu.co

16.11Criterio Diferencial de Accesibilidad

Con el objeto de facilitar que todas las personas sin distinción alguna puedan acceder a la información que particularmente les afecte, el Servicio Nacional de Aprendizaje SENA, divulgará y adecuará sus documentos y formatos de manera progresiva, a diversos idiomas y lenguas; asegurando el acceso a la información de los distintos grupos étnicos y culturales del país, así como la adecuación de los medios de comunicación, para facilitar y garantizar el acceso a personas con discapacidad, en cumplimiento a lo establecido en el artículo 8 de la Ley 1712 de 2014..

16.12 Procedimiento para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar

Los titulares o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la Ley y demás normas que la desarrollan, podrán presentar un reclamo que deberá contener como mínimo la siguiente información, siguiendo los medios y procedimientos que el SENA destine para este.

- Identificación del titular del dato.

- Descripción precisa de los hechos que dan lugar al reclamo.

- Datos de notificación, dirección física y/o electrónica.

- Los demás documentos que se quiera hacer valer.

- Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

- En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

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

- El reclamo será atendido dentro de los quince (15) días hábiles, contados a partir del día siguiente a la fecha de su recibo. Si no fuere posible atender el reclamo dentro del término

establecido, el SENA informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar a ocho (8) días hábiles siguientes al vencimiento del primer término.

16.13 Derecho de acceso a los datos personales

El SENA garantiza el derecho de acceso a los datos personales, a las siguientes personas:

- A los Titulares, sus causahabientes o sus representantes legales quienes deberán acreditar tal calidad.

- A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.

- A los terceros autorizados por el Titular o por la ley.

Para tal efecto se garantiza el establecimiento de medios y mecanismos electrónicos y/o presenciales con disponibilidad permanente, los cuales permitan el acceso directo del titular a los datos personales, los cuales serán informados en el Aviso de Privacidad o en el Formato de Autorización para el tratamiento de datos personales.

De acuerdo con lo previsto en la normatividad aplicable, para el ejercicio de los derechos que le asisten como titular de los datos, las personas anteriormente señaladas podrán hacer uso ante el Servicio Nacional de Aprendizaje SENA, de los siguientes mecanismos:

16.13.1 Derecho de consulta de información personal

- Los titulares, causahabientes o sus representantes, que acrediten tal calidad, podrán consultar la información personal del titular que repose en cualquier base de datos, por lo que el SENA como responsable del tratamiento, suministrará a éstos, toda la información contenida en el registro individual o que esté vinculada con la identificación del titular.

- El SENA garantiza los medios de comunicación electrónica para la formulación de consultas, los cuales serán los mismos utilizados para la recepción y atención de peticiones, quejas, reclamos y sugerencias, administrado por la Coordinación Nacional de Servicio al Ciudadano.

- La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

16.13.2 Derecho de actualización y rectificación de datos

- El SENA, como responsable del tratamiento de los datos, deberá rectificar y actualizar a solicitud del titular toda información que resulte ser incompleta o inexacta. Para estos efectos, el titular o su causahabiente y/o representante, señalará las actualizaciones y rectificaciones a que dieran lugar, junto a la documentación que soporte su solicitud.

- El SENA habilitará los medios electrónicos existentes en la Entidad encaminados a garantizar este derecho, que serán los mismos utilizados para la recepción y atención de peticiones, quejas, reclamos y sugerencias, administrado por la Coordinación Nacional de Servicio al Ciudadano.

16.13.3 Derecho a solicitar la supresión de datos personales

- Los Titulares podrán solicitar al SENA la supresión de sus datos personales mediante la presentación de un reclamo, cuando consideren que los datos no están recibiendo un tratamiento adecuado, o los mismos no son pertinentes o necesarios con la finalidad para la cual fueron recolectados.

- No obstante, la solicitud de supresión de datos no procederá cuando el titular tenga un deber legal o contractual de permanecer en la(s) base(s) de datos o la supresión de los datos represente un impedimento en actuaciones administrativas o judiciales relacionadas con obligaciones fiscales, investigación de delitos o actualización de sanciones administrativas.

- Si vencido el término legal respectivo, no se han eliminado los datos personales, el titular tendrá derecho a solicitar a la Superintendencia de Industria y Comercio que ordene la supresión de los datos personales.

- El SENA garantiza los medios de comunicación electrónica u otros para solicitud de supresión de datos, que serán los mismos utilizados para la recepción y atención de peticiones, quejas, reclamos y sugerencias, administrado por la Coordinación Nacional de Servicio al Ciudadano.

16.14 Vigencia y aviso de posible cambio sustancial en las políticas de tratamiento

- La presente Política para el Tratamiento de Datos Personales rige a partir de la fecha de su publicación en el diario oficial, se divulgará a través del portal institucional, y estará sujeto a actualizaciones en la medida en que se modifiquen o se dicten nuevas disposiciones legales sobre la materia.

- Cuando se cumplan estas condiciones, el SENA informará a los titulares de los datos personales, sus causahabientes o representantes, las nuevas medidas dictadas, antes de su implementación. Además, deberá obtener del titular una nueva autorización cuando el cambio se refiera a la finalidad del tratamiento.

17 Glosario de Términos

- Activo: Se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tienen un valor para la entidad.

- Activo crítico: Instalaciones, sistemas y equipos los cuales, si son destruidos, o es degradado su funcionamiento o por cualquier otro motivo no se encuentran disponibles, afectaran el cumplimiento de los objetivos misionales del Sena.

- Administración de Riesgos: Se entiende por administración de riesgos, como el proceso de identificación, control, minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar la información o impactar de manera considerable la operación. Dicho proceso es cíclico y deberá llevarse a cabo en forma periódica.

- Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.

- Análisis de Impacto al Negocio: Es una metodología que permite identificar los procesos críticos que apoyan los productos y servicios claves, las interdependencias entre procesos, los recursos requeridos para operar en un nivel mínimo aceptable y el efecto que una interrupción

del negocio podría tener sobre ellos.

- Áreas Seguras: Son aquellas en donde se encuentren sistemas de procesamiento y almacenamiento informático o de datos. En el Sena se identifican las siguientes áreas seguras:

- Cuarto de cableado.

- Centro de datos.

- Archivos generales y de gestión.

- Lugares que contengan información Reservada (oficinas con expedientes, registros de aprendices, entre otros).

- Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

- Centro de cableado: el centro de cableado es el lugar donde se ubican los recursos de comunicación de Tecnología de información, como (Switch, patch, panel, UPS, Router, Cableado de voz y de datos).

- Ciberactivo crítico: Ciberactivo que es crítico para la operación de un activo crítico.

- Ciberactivo: Se identifica como foco de la ciberseguridad los activos digitales como datos, dispositivos y sistemas que permiten a la organización cumplir con sus objetivos de negocio.

- Ciberseguridad: Es el proceso de proteger los activos de información por medio del tratamiento de las amenazas a la información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.

- Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

- Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

- CCOCI: Comando Conjunto Cibernético, Unidad Militar Conjunta (Ejército, Armada y Fuerza Aérea), que tiene como función principal prevenir, detectar, orientar, contener, decidir, responder y recuperar ante amenazas cibernéticas que afecten la sociedad, la soberanía nacional, independencia, integridad territorial, el orden constitucional y los intereses nacionales, todo esto, soportado en un marco jurídico y/o la Constitución Nacional.

- COLCERT: Por las siglas en inglés de Computer Emergency Response Team, es el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, y tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual estará enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal será la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de Ciberseguridad que atenten o comprometan la seguridad y defensa nacional.

- CSIRT: Por las siglas en inglés de Computer Security Incident Response Team, es el equipo de Respuesta a Incidentes de Seguridad Informática.

- Datacenter: Se denomina también Centro de Procesamiento de Datos (CPD) a aquella ubicación o espacio donde se concentran los recursos necesarios (TI) para el procesamiento de la información de una organización.

- Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

- Dispositivos móviles: equipo de cómputo pequeño, cuyo concepto principal es la movilidad, el cual permite almacenamiento limitado, acceso a internet y cuenta con capacidad de procesamiento.

- DMZ: Sigla en inglés de DeMilitarized Zone hace referencia a un segmento de la red que se ubica entre la red interna de una organización y la red externa o internet de VPN.

- Equipos activos de red: son todos los dispositivos que hacen la distribución de las comunicaciones a través de la red de datos del Sena.

- Evaluación de Riesgos: Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operación de la entidad.

- Incidente de Seguridad: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información.

- Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

- Infraestructura Crítica (IC): Son las infraestructuras estratégicas cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. Adaptación Ley 8/2011-Gobierno de España.

- Infraestructura Crítica Cibernética (ICC): Son las infraestructuras estratégicas soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO), cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. Fuente: Ministerio de Defensa.

- Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

- Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la entidad.

- Medio removible: Los dispositivos de almacenamiento removibles son dispositivos de almacenamiento independientes del computador y que pueden ser transportados libremente. Los dispositivos móviles más comunes son: Memorias USB, Discos duros extraíbles, DVD y CD.

- Mesa de Servicio: Constituye el único punto de contacto con los usuarios finales para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de

servicio y solicitudes de información.

- No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

- Paneles de conexión (patch panel): Elemento encargado para la organización de conexiones en la red.

- Plan de Continuidad de Negocio: Actividades documentadas que guían a la Entidad en la respuesta, recuperación, reanudación y restauración de las operaciones a los niveles predefinidos después de un incidente que afecte la continuidad de las operaciones.

- Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

- Propietario del riesgo: Persona o proceso con responsabilidad y autoridad para gestionar un riesgo.

- Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

- Responsable de Seguridad de la información: Es la persona que cumple la función de supervisar el cumplimiento de la presente Política, coordinar el Comité de Seguridad de la Información y de asesorar en la materia a los integrantes de la entidad que así lo requieran.

- Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

- Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales. Conjunto de aplicaciones que interactúan entre sí para apoyar un área o proceso del Sena.

- Tecnología de la Información: Las tecnologías de la información y las Comunicaciones (TIC o TICs), Nuevas Tecnologías de la Información y de la Comunicación (NTIC), agrupan los elementos y las técnicas utilizadas en el tratamiento y la transmisión de las informaciones, principalmente de informática, internet y telecomunicaciones.

- Test de penetración: es un ataque dirigido y controlado hacia componentes de infraestructura tecnológica para revelar malas configuraciones y vulnerabilidades explotables.

- VPN: red virtual privada por sus siglas en ingles Virtual Private Network.

SERVICIO NACIONAL DE APRENDIZAJE SENA

FORMATO DE MEMORIA JUSTIFICATIVA

1.Proyecto de Normatividad	Acuerdo del Consejo Directivo Nacional para la Aprobación de la Política General de Seguridad de la Información y Protección de Datos Personales en el SENA
2.Dependencia o Grupo responsable	Dirección de Planeación y Direccionamiento Corporativo
3.Fecha de elaboración	8 de noviembre de 2019
4. Documentos base aportados	Constitución Política Ley 1266 de 2008 Ley Estatutaria 1581 de 2012 Decreto 1377 de 2013 Ley 1712 de 2014 Decreto Único Reglamentario 1081 de 2015 del Sector Presidencial de la República, compiló el Decreto 103 de 2015 Conpes 3854 de 2016 Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018 Norma Técnica NTC-ISO-IEC27001 Acuero 09 de 2016

I, ANTECEDENTES, OPORTUNIDAD Y CONVENIENCIA

1.1 ANTECEDENTES:

El artículo 1 de la Ley 119 de 1994, dispone: “NATURALEZA. El Servido Nadonol de Aprendizaje, SENA, es un establedmiento público del orden nacional con personería jurídica, patrimonio propio e independiente, y autonomía administrativa, adscrito al Ministerio de Trabajo y Seguridad Sociar, hoy Ministerio del Trabajo.

1. 2. OBJETO SOCIAL DEL SENA:

La Constitución Política de Colombia señala en su articulo 115 que los establecimientos públicos y las empresas industriales o comerciales del Estado, forman parte de la Rama Ejecutiva", y agrega en su articulo 150 - numeral 7 que corresponde al Congreso mediante ley “determinar la estructura de la administración nacional y crear, suprimir o fusionar (...) establecimientos públicos y otras entidades del orden nacional, señalando sus objetivos y estructura orgánica."

Por su parte, la Ley 489 de 1998 "Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del articulo 189 de la Constitución Política y se dictan otras disposiciones", define el objeto social de los establecimientos públicos, como el SENA, indicando:

"Artículo 70. Establecimientos públicos. Los establecimientos públicos son organismos encargados principalmente de atender funciones administrativas y de prestar servicios públicos conforme a las reglas del Derecho Público, que reúnen las siguientes características:

a) Personería jurídica;

b) Autonomía administrativa y financiera;

c) Patrimonio independiente, constituido con bienes o fondos públicos comunes, el producto de impuestos, rentas contractuales, ingresos propios, tasas o contribuciones de destinación especial, en los casos autorizados por la Constitución y en las disposiciones legales pertinentes."

"Artículo 71. Autonomía administrativa y financiera. La autonomía administrativa y financiera de los establecimientos públicos se ejercerá conforme a los actos que los rigen y en el cumplimiento de sus funciones, se ceñirán a la ley o norma que los creó o autorizó y a sus estatutos internos; y no podrán desarrollar actividades o ejecutar actos distintos de los allí previstos ni destinar cualquier parte de sus bienes o recursos para fines diferentes de los contemplados en ellos."

Como se observa, la naturaleza jurídica del SENA enmarca su accionar y la dinámica organizadonal de la entidad; dicho marco constitucional y legal implica tener un régimen jurídico propio, autonomía administrativa y la facultad de cumplir sus funciones conforme a la ley o norma que lo crea y a sus estatutos internos.

Por su parte, el legislador le asignó al SENA en el artículo 4® de la misma Ley 119 de 1994, las siguientes funciones:

“ARTÍCULO 4o. Funciones. Son funciones del Servicio Nacional de Aprendizaje, SENA, los siguientes:

1. Impulsar la promoción social del trabajador, a través de su formación profesional integral, para hacer de él un ciudadano útil y responsable, poseedor de valores morales éticos, culturales y ecológicos.

2. Velar por el mantenimiento de los mecanismos que aseguren el cumplimiento de las disposiciones legales y reglamentarias, relacionadas con el contrato de aprendizaje.

3. Organizar, desarrollar, administrar y ejecutor programas de formación profesional integral, en coordinación y en función de las necesidades sociales y del sector productivo.

4. Velar porque en los contenidos de los programas de formación profesional se mantengo la unidad técnico.

5. Crear y administrar un sistema de información sobre oferta y demondo laboral.

6. Adelantar programas de formación tecnológica y técnica profesional, en los términos previstos en las disposiciones legales respectivas.

7. Diseñar, promover y ejecutar programas de formación profesional integral para sectores desprotegidos de la población.

8. Dar capacitación en aspectos socio empresariales a los productores y comunidades del sector informal urbano y rural.

9. Organizar programas de formación profesional integral para personas desempleadas y subempleadas y programas de readaptación profesional para personas discapacitadas.

10. Expedir títulos y certificados de los programas y cursos que imparta o valide, dentro de los campos propios de ia formación profesional integral, en los niveles que los disposiciones legales le autoricen. GJ-F-003-V02

11. Desarrollar investigaciones que se relacionen con la organización del trabajo y el avance tecnológico del país, en función de los programas de formación profesional.

12. Asesorar al Ministerio de Trabajo y Seguridad Social en la realización de investigaciones sobre recursos humanos y en la elaboración y permanente actualización de la clasificación nacional de ocupaciones, que sirva de insumo a la planeación y elaboración de planes y programas de formación profesional integral.

13. Asesorar al Ministerio de Educación Nacional en el diseño de los programas de educación media técnica, para articularlos con la formación profesional integral.

14. Prestar servicios tecnológicos en función de la formación profesional integral, cuyos costos serán cubiertos plenamente por los beneficiarios, siempre y cuando no se afecte la prestación de los programas de formación profesionar.

Lo anterior es consecuente con el artículo 54 de la Constitución Política, que establece:

"ARTICULO 54. Es obligación del Estado y de los empleadores ofrecer formación y habilitación profesional y técnica a quienes lo requieran. El Estado debe propiciar la ubicación laboral de las personas en edad de trabajar y garantizar a los minusválidos el derecho a un trabajo acorde con sus condiciones de salud". (Resaltado propio)

Otras disposiciones legales le asignan al SENA funciones específicas, como las siguientes:

- la Ley 1636 de 2013 *Por medio de la cual se crea el mecanismo de protección al cesante en Colombia", establece en su artículo 28 que le corresponde al SENA prestar "los servicios de gestión y colocación de empleo" a través de la Agencia Pública de Empleo a cargo del Servicio Nacional de Aprendizaje Sena", junto con las agencias públicas y privadas de gestión y colocación de empleo y las bolsas de empleo, que cumplan los requisitos de operación y desempeño que definael Ministerio del Trabajo para su autorización".

- La Ley 1286 de 2009 "Por la cual se modifica la Ley 29 de 1990, se transforma a Colciencias en Departamento Administrativo, se fortalece el Sistema Nacional de Ciencia, Tecnología e Innovación en Colombia y se dictan otras disposiciones", señala en su artículo 33 que el SENA debe destinar recursos "para el desarrollo de la ciencia, tecnología e innovación acorde con los objetivos" de esta entidad.

- En materia de emprendimiento, la misma Ley 789 de 2002 le asignó al SENA la administración del Fondo Emprender - FE, señalando en su artículo 40 lo siguiente: "Fondo Emprender. Créase el Fondo Emprender, FE, como una cuenta independiente y especial adscrita al Servicio Nacional de Aprendizaje, SENA, el cual será administrado por esta entidad y cuyo objeto exclusivo será financiar iniciativas empresariales que provengan y sean desarrolladas por aprendices o asociaciones entre aprendices, practicantes universitarios o profesionales que su formación se esté desarrollando o se hoya desarrollado en instituciones que para los efectos legales, sean reconocidas por el Estado de conformidad con las Leyes 30 de 1992 y 115 de 1994 y demás que las complementen, modifiquen o adicionen. // (...)"

Las funciones asignadas por el legislador al SENA evidencian el amplio campo de acción que tiene esta entidad, además de ser una institución que tiene cobertura y presencia nacional, con 33 Regionales y 117 Centros de Formación y que, de acuerdo con su marco normativo, el SENA cumple las siguientes funciones:

- Ofrece y desarrolla programas de formación en los siguientes niveles:

-- No formal
-- Capacitación.

-- Educación para el trabajo y el desarrollo humano.

-- Integración técnica con la educación media.

-- Educación superior.

-- Especializaciones técnicas y tecnológicas.

- Normaliza competencias laborales.

- Evalúa y certifica competencias laborales.

- Presta servicios de Agencia Pública de Empleo.

- Realiza y promueve la investigación, la innovación y el desarrollo tecnológico.

- Presta servicios técnicos y tecnológicos a las empresas.

- Promueve y financia el emprendimiento y empresarismo.

- Atiende poblaciones especiales.

- Asesora y asiste a las empresas.

- Expide regulaciones normativas como en materia de contrato de aprendizaje y multas.

- Realiza la parte operativa del contrato de aprendizaje.

- Desarrollo de la Normatividad propia para la administración de la Entidad.

Esta variedad de programas que ofrece el SENA y de funciones asignadas por la ley, le implica a la entidad y a su personal, cumplir con diferentes niveles de exigencia y de regímenes normativos, de acuerdo con las disposiciones que reglamentan esos programas o funciones, y las propias de la Entidad.

Es así, que el SENA, como entidad pública adscrita al Ministerio del Trabajo, dispone de un marco legal aplicable conforme a las leyes vigentes y un marco de referencia basado en estándares y buenas prácticas de seguridad, con el objetivo de proteger y preservar los activos de información, se hace necesario desarrollar e implementar el modelo de seguridad y privacidad de la información y el SGSI de la entidad, dando cumplimiento tanto a lo consagrado en la Constitución Política como en las disposiciones normativas que se han expedido para este fin. Entre ellas, tenemos:

Constitución Política de Colombia, artículo 15: "todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. // En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada

son inviolables. Solo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley (...)"

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.

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.

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 de datos den cabal cumplimiento a las mismas.

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 dispone que el objeto de la ley, 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 que "constituye el marco general de la protección del ejercicio del derecho de acceso a la información pública en Colombia".

El Decreto Único Reglamentario 1081 de 2015 del Sector Presidencia de la República, compiló el Decreto 103 de 2015 por el cual se reglamenta parcialmente la Ley 1712 de 2014, el cual establece los temas relacionados con la gestión de la información pública, 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.

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.

El documento Conpes 3854 de 2016, establece la Política Nacional de Seguridad Digital en la República de Colombia.

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

en el SENA, 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 la Norma Técnica NTC- ISO-IEC 27001 del 2013 contempla los lincamientos a tener en cuenta en el diseño de las políticas en: Las Tecnologías de la Información, Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información.

Que el documento CONPES 3975 expedido en noviembre de 2019, establece la Política Nacional para la transformación digital e inteligencia artificial.

Así mismo, en el Plan Nacional de Desarrollo 2018*2022 "Pacto por Colombia, pacto por la equidad" reglamentado a través de la Ley 1955 de 2019 señala en su artículo 147que: "Transformación Digital Pública. Las entidades estatales del orden nacional deberán incorporar en sus respectivos planes de acción el componente de transformación digital siguiendo los estándares que para este propósito defina el Ministerio de Tecnologías de la Información y las Comunicaciones. En todos los escenarios la transformación digital deberá incorporar los componentes asociados a tecnologías emergentes, definidos como aquellos de la Cuarta Revolución Industrial, entre otros. (...)"

Por lo anteriormente expuesto, la necesidad del Servicio Nacional de Aprendizaje y el compromiso de la Alta Dirección- SENA, encaminado a definir las bases de gobernanza para gestionar y preservar de manera efectiva la confidencialidad, integridad, disponibilidad y privacidad de sus activos de información de propiedad del SENA por parte de la comunidad SENA y de terceros, aprobó emitir la Política General de Seguridad de la Información en el SENA y así quedó consignado en el acta 19 del Comité Directivo y Comité Institucional de Gestión y Desempeño del 28 de mayo de 2019. Indicando la necesidad 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 lincamientos 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.

2. RAZONES DE OPORTUNIDAD Y CONVENIENCIA:

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 y mitigar el riesgo antijurídico en el manejo de la misma.

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 General de Seguridad de la Información y Protección de Datos Personales del SENA aplica a todos los funcionarios, contratistas, aprendices y terceros que tengan o soliciten acceso a información a través de cualquier medio.

III. VIABILIDAD JURÍDICA

1. Análisis de normas que otorgan competencia para la expedición del acto	Atendiendo la necesidad de contar con una política de seguridad de la información y protección de datos personales en el SENA, las competencias para que esta se expida es de resorte del Consejo Directivo Nacional, como máximo Organismo de la Entidad, conferidas en la Ley 119 de 1994 y el Decreto 249 de 2004, señalados en los siguientes artículos: Articulo 10 Ley 119 de 1994. Funciones del Consejo Directivo Nacional: "1. Definir y formular la política general y los planes y programas de la entidad. Articulo 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. (...) 27. Las demás que le sean asignadados. PARÁGRAFO. El Consejo Directivo Nacional podrá delegar en el Director General las funciones que considere convenientes, de conformidad con las reglas de delegación contenidas en la Ley 489 de 1998, o las normas que la modifiquen". De igual manera atendiendo las disposiciones antes señaladas podrá delegar en el Director General como Representante Legal el desarrollo de las políticas complementarias para dar plena aplicabilidad a la política que aquí se aprueba
2. La vigencia de la ley o norma reglamentada o desarrollada	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. El Decreto 1377 de 2013, "por el cual se reglamenta parcialmente la Ley 1581 de 2012*, establece en su articulo 13 que los responsables del tratamiento de la información deberán desarrollar sus políticas para el tratamiento de los datos personales y velar porque los en cargados del tratamiento de datos den cabal cumplimiento a las mismas. 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 dispone que el objeto de la ley, 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 que 'constituye el marco general de la protección del ejercicio del derecho de acceso a la información pública en Colombia'. El Decreto Único Reglamentario 1081 de 2015 del Sector Presidencia de la República, compiló el Decreto 103 de 2015 por el cual se reglamenta parcialmente la Ley 1712 de 2014, el cual establece los temas relacionados con la gestión de la Información pública, 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, asi como el seguimiento de la misma. El Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, en el articulo 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 articulo 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 la Norma Técnica NTC- ISO-IEC 27001 del 2013 contempla los lineamientos a tener en cuenta en el diseño de las políticas en: Las Tecnologías de la Información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información El documento Conpes 3854 de 2016, establece la Política Nacional de Seguridad Digital en la República de Colombia. El documento Conpes 3975, establece la Política Nacional para la transformación digital e inteligencia artificial, del 8 de noviembre de 2019.
3. Disposiciones derogadas, subrogadas, modificadas, adicionadas o sustituidas, estos efectos se producen con la expedición respectivo acto	Para los efectos de la aplicación del presente acuerdo, y de manera transitoria se mantendrá vigente el acuerdo 009 de 2016 y su instructivo de Política de Protección de Datos personales, mientras se desarrollan las Políticas complementarias de tratamiento de Datos personales en la Entidad. Asi mismo; dentro Acuerdo, se le da facultad al Director General del Sena para que, a través de acto administrativo, apruebe y adopte las políticas complementarias necesarias para garantizar la implementación del Manual de Seguridad de la Información y Protección de Datos Personales en el 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	N/A.
5. Otras circunstancias jurídicas relevantes para la expedición del acto	N/A.

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 tiene afectación presupuestal.

VI. IMPACTO MEDIOAMBIENTAL O SOBRE EL PATRIMONIO CULTURAL DE LA NACIÓN

La expedición e implementación del acuerdo no qenera impacto ambiental ni sobre el patrimonio cultural de la Nación.

VIl. CONSULTAS y PUBLICIDAD

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

2. Publicidad: en cumplimiento de lo dispuesto en el numeral 6 del articulo 3* y el numeral 8 del articulo 8 de la Ley 1437 de 2011, y en concordancia con lo previsto en el articulo 2.1.2.1.14 del Decreto 1609 de 2015, el texto del presente acto administrativo se publicó los dias 9 al 11 de octubre de 2019 y 12 al 14 de noviembre del mismo año. en la página web del SENA para comentarios de la ciudadanía para lo cual se solicitó a la Dirección Jurídica proceder de conformidad: quien mediante radicados 8-20194)71178 y 8-2019-081704 respectivamente ordenó realizar la publicación ante la Oficina de Comunicaciones del SENA.

Las observaciones y sugerencias recibidas fueron debidamente analizadas e incorporadas en el manual atendiendo 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

SI las hubo debe decirse cuales fueron las más relevantes.

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 articulo 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 y las observaciones y sugerencias recibidas fueron debidamente analizadas e incorporadas en el manual atendiendo su pertinencia.

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

SI__ NO__

XIII. ANEXOS

Juan Fernando Lopez Mejia
Director De la Direccion de Planeación y Direccionamiento Corporativo

NOTAS AL FINAL:

1 Definición de servidor pública contenida en el Decreto 1083 de 2015.

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)