PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Enero de 2023

Dirección General
Calle 57 No. 8 - 69 Bogotá D.C. (Cundinamarca)-PBX 57 601 5461500

@SENAComunica
www.sena.edu.co

TABLA DE CONTENIDO

Dirección General
Calle 57 No. 8 - 69 Bogotá D.C. (Cundinamarca)-PBX 57 601 5461500
@SENAComunica
www.sena.edu.co

1. INTRODUCCIÓN

El Modelo de Seguridad y Privacidad de la Información - MSPI, es el instrumento a través del cual el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, establece los lineamientos que deben seguir las entidades públicas en cumplimiento de la política de gobierno digital en su habilitador transversal “Seguridad de la información”, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.

El Servicio Nacional de Aprendizaje - SENA reconoce la importancia y el valor de los activos (en especial de la información) tanto para el funcionamiento al interior de la entidad como de cara a los ciudadanos y así mismo reconoce que deben protegerse de los posibles riesgos a los que puedan verse expuestos.

A fin de garantizar los principios de integridad, confidencialidad, disponibilidad y mitigar los posibles riesgos que puedan afectar a los activos, el Servicio Nacional de Aprendizaje - SENA ha decidido implementar un Sistema de Gestión de Seguridad y Privacidad de la Información, de acuerdo con la normatividad vigente, estableciendo directrices en el marco de la transformación digital que permita maximizar la efectividad en los procesos y minimizar la exposición al riesgo derivado del uso de tecnologías de la información y las comunicaciones.

Por tanto, el presente documento define la hoja de ruta a seguir en el Servicio Nacional de Aprendizaje – SENA, acorde con lo establecido en la Norma Técnica Colombiana NTC IEC/ISO 27001:2013 aplicando el ciclo de mejora continua y lo establecido para la gestión de seguridad y privacidad de la información en la vigencia 2023.

2. OBJETIVO GENERAL

Establecer las actividades necesarias para el fortalecimiento del sistema de gestión de Seguridad y Privacidad de la Información, alineado con la NTC/IEC ISO 27001:2013, la Política de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones, la Política de Seguridad y Privacidad de la Información y Seguridad Digital en el Servicio Nacional de Aprendizaje - SENA y el Modelo Integrado de Planeación y Gestión - MIPG.

3. OBJETIVOS ESPECÍFICOS

- Definir las actividades que darán cumplimiento a las (5) cinco fases del Modelo de Seguridad y Privacidad de la Información tales como: Diagnóstico, Planificación, Operación, Evaluación de desempeño y Mejoramiento continuo.
- Dar cumplimiento a los requisitos legales y normativos en materia de seguridad y privacidad de la información, seguridad digital y protección de la información personal.

- Dar garantías a la ciudadanía de la Custodia de la información que reposa en el Servicio Nacional de Aprendizaje - SENA a través de la implementación de controles de seguridad de la información soportados en la confidencialidad, integridad y disponibilidad.
- Incrementar el nivel de madurez del Modelo de Seguridad y Privacidad de la Información en el Servicio Nacional de Aprendizaje - SENA.
- Fomentar una cultura institucional en donde se sensibilice a los funcionarios y contratistas del Servicio Nacional de Aprendizaje - SENA acerca del Sistema de Gestión de Seguridad de la Información y el modelo de Privacidad de la información.
- Orientar en la adopción y aplicación de la legislación relacionada con la protección de datos personales.

4. ALCANCE

El Plan de Seguridad y Privacidad de la Información y Seguridad Digital, aplica para todos los procesos, direcciones, oficinas, regionales y centros de formación, y es de obligatorio complimiento para los funcionarios, contratistas, instructores, aprendices y terceros que tengan vínculos laborales, de formación o contractuales con la entidad y que en razón del cumplimiento de sus funciones compartan, utilicen, recolecten, procesen, intercambien o consulten su información de forma interna o externa, independientemente de su ubicación. De igual forma, esta política aplica a toda la información creada, procesada o utilizada por la entidad, sin importar el medio, formato, presentación o lugar en la cual se encuentre.

5. REFERENCIAS NORMATIVAS

El diseño e implementación del Sistema de Gestión de Seguridad de la Información – SGSI del Servicio Nacional de Aprendizaje - SENA se basa en la normatividad exigida por el Ministerio de Tecnologías de la Información y Comunicaciones – MINTIC.

- Ley 1581 de 2012 del Congreso de la República, *“Por la cual se dictan disposiciones generales para la protección de datos personales”*.
- Decreto 2609 de 2012 de la Presidencia de la República, *“Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado”*.
- Decreto 1377 de 2013 del Ministerio de Comercio, Industria y Turismo, *“Por el cual se reglamenta parcialmente la Ley 1581 de 2012”*.
- Decreto 612 de 2018 de la Presidencia de la República, “*Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado”.*
- Decreto 886 de 2014 del Ministerio de Comercio, Industria y Turismo, *“Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos”*.

Dirección General
Calle 57 No. 8 - 69 Bogotá D.C. (Cundinamarca)-PBX 57 601 5461500
@SENAComunica
www.sena.edu.co

- Ley 1712 de 2014 del Congreso de la República, *"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"*.
- NTC-ISO/IEC 27001:2013, Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la seguridad de la información (SGSI). Requisitos (ISO/IEC 27001:2013 – *Information technology – Security techniques – Information security management systems – Requirements*).
- Decreto 103 de 2015 de la Presidencia de la República, *"Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones*".
- Decreto 1008 de 2018 del Ministerio de Tecnologías de la Información y las Comunicaciones, *"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".*
- Decreto 1083 de 2015 del Departamento Administrativo de la Función Pública, *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública",* el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de *"11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital"*.
- Modelo Integrado de Planeación y Gestión – MIPG versión 4, marzo de 2021.
- Decreto 2106 de 2019 del Departamento Administrativo de la Función Pública, *"Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública*", en el cual se establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.
- Resolución 0500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones, *"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".*
- Modelo de Seguridad y Privacidad de la Información (MSPI), Política de Gobierno Digital, Ministerio de Tecnologías de la Información y las Comunicaciones – versión 4. 2021.
- CONPES 3995 de 2020 - Política Nacional de Confianza y Seguridad Digital.
- Resolución 0083 de 2021 del Servicio Nacional de Aprendizaje - SENA, "Por la cual se adopta la Política General de Seguridad y Privacidad de la Información y Seguridad Digital del Servicio Nacional de Aprendizaje - SENA y se deroga la Resolución No. 0635 del 12 de abril de 2017".

Dirección General
Calle 57 No. 8 - 69 Bogotá D.C. (Cundinamarca)-PBX 57 601 5461500
@SENAComunica
www.sena.edu.co

6. DESCRIPCIÓN GENERAL DEL DISEÑO, IMPLEMENTACIÓN Y DOCUMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA ENTIDAD

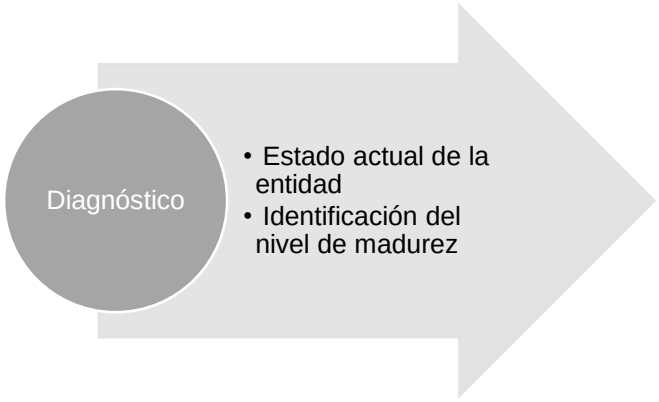
Para llevar a cabo el proyecto de diseño, implementación y documentación del sistema gestión de seguridad y privacidad de la información del Servicio Nacional de Aprendizaje - SENA, se deben ejecutar las siguientes fases:

6.1. **Diagnóstico**

Anualmente se realiza el Autodiagnóstico de la Política de Seguridad de la Información el cual se desarrolla de acuerdo con los lineamientos de MINTIC, así como el GAP (metodología de Diagnóstico, Priorización, Planificación y Reevaluación.), el cual incluye los requerimientos relacionados con la seguridad y privacidad de la información.

A partir del autodiagnóstico se analiza las acciones que permitan cerrar estas brechas, el cual se realiza, comparando el desempeño real de la entidad en cuanto al cumplimiento de la norma ISO 27001 frente a la adopción del MSPI. (Modelo de seguridad y privacidad de la información).

Figura 1. Fase de diagnóstico[1]



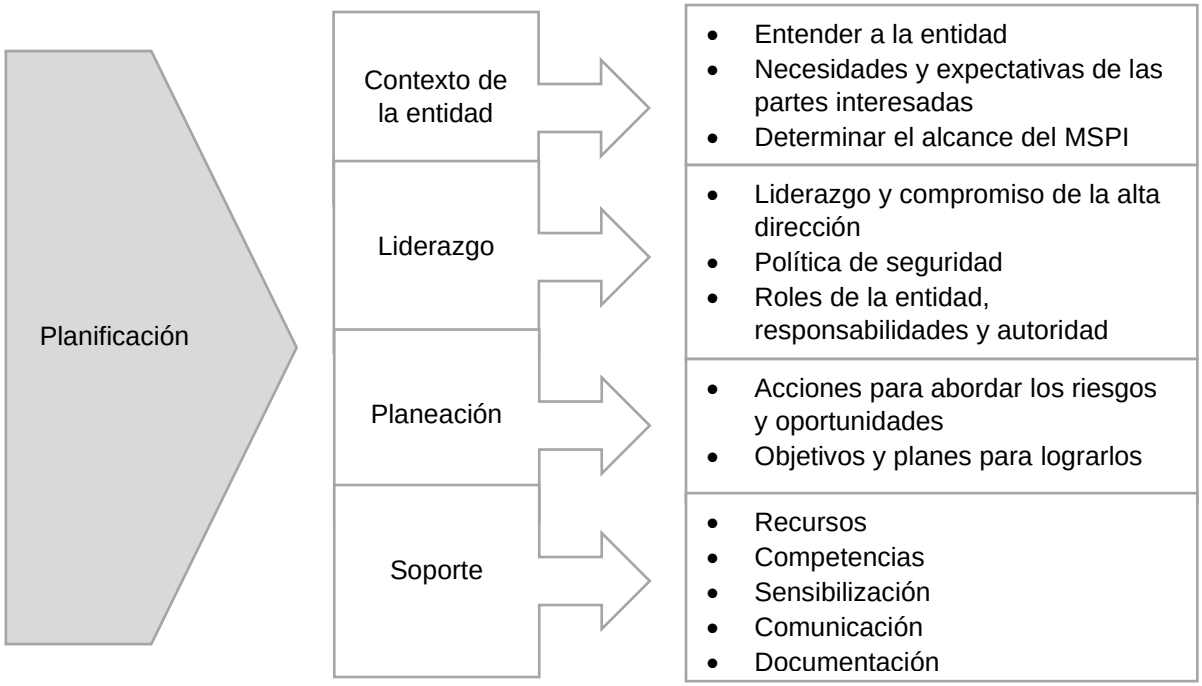
6.2. **Planificación**

De acuerdo con el resultado de la fase de diagnóstico, se definen las necesidades y objetivos de seguridad y privacidad de la información basados en el contexto estratégico, el modelo de operación del SENA, los recursos disponibles y su articulación con el Plan Estratégico

[1] Adaptado del Modelo de Seguridad y Privacidad de la Información - MINTIC

Institucional, entre otros, los cuales permiten definir los lineamientos para asegurar el cumplimiento de los requisitos de Modelo de Seguridad y Privacidad de la Información. Los aspectos que se tienen en cuenta para las planeación del Modelo de Seguridad y Privacidad de la información se muestran a continuación:

Figura 2. Fase de planificación[2]

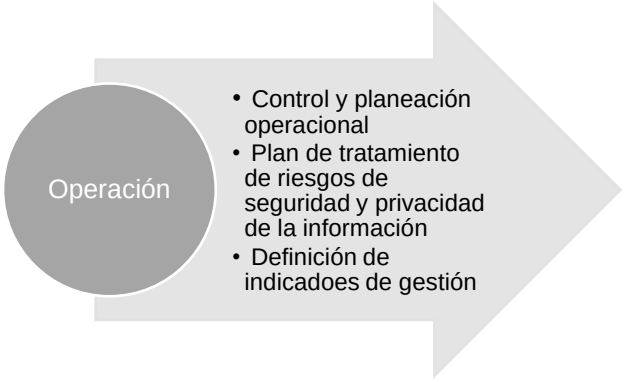


6.3. **Operación**

Es necesario desarrollar la implementación de la política general de seguridad y privacidad de la información a través de la estructuración y puesta en marcha de los controles de seguridad de la información que ayudan a mitigar el impacto de los riesgos definidos en la etapa de Planificación que hacen parte del Modelo de Seguridad y Privacidad de la Información.

[2] Ibid.

Figura 3. Fases de Operación[3]



6.4. **Evaluación de desempeño**

La evaluación del desempeño del Modelo de Seguridad y Privacidad de la información, se realiza a través de la medición y monitoreo de los indicadores de gestión, el seguimiento de la eficacia de los controles para determinar su efectividad, la revisión por la Alta Dirección del SENA para determinar las acciones necesarias que permitan mejorar la implementación su implementación y finalmente la auditorías internas.

Con la revisión periódica se debe asegurar que las mejoras realizadas cumplan con los objetivos dispuestos en la Política de Seguridad y Privacidad de la Información y Seguridad Digital.

Figura 4. Fase Evaluación de desempeño[4]

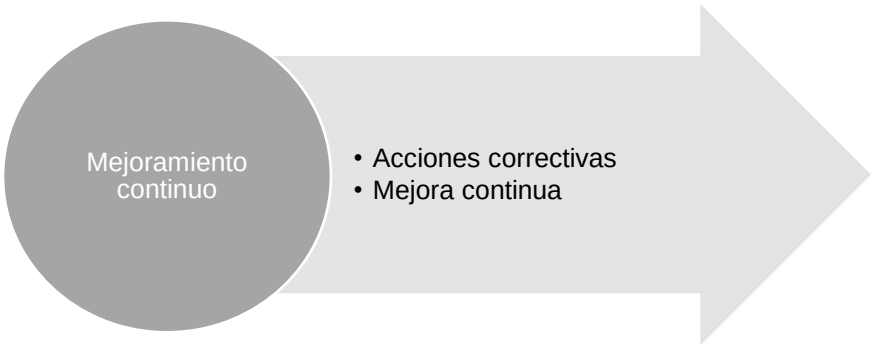
[3] Adaptado del Modelo de Seguridad y Privacidad de la Información - MINTIC
[4] Ibid.

6.5. **Mejoramiento Continuo**

El mejoramiento continuo del Modelo de Seguridad y Privacidad de la información es el resultado del seguimiento y revisión de todo el sistema de seguridad y privacidad de la información, donde se evalúa el alcance, la metodología de riesgo y la eficacia de los controles, que como resultado se identifican mejoras al sistema a través de planes de mejoramiento (acciones correctivas) y de esta manera mejorar continuamente el desempeño institucional del citado Modelo.

Resultado del mejoramiento continuo, se retroalimentan los planes de seguridad, políticas, procedimientos y controles, que impacta de manera positiva, en el desempeño del sistema.

Figura 5. Fase Mejora Continua[5]



6.6. **Plan de Implementación del Modelo de Seguridad y Privacidad de la Información**

El Plan de implementación para el modelo de Seguridad y Privacidad de la Información para el Servicio Nacional de Aprendizaje - SENA, comprende el siguiente cronograma el cual tendrá seguimiento trimestral:

Tabla 1. Plan de implementación para el modelo de Seguridad y Privacidad de la Información parea el SENA 2023

Fase	Actividad	Responsable	Entregable	Fecha Programación	
				Fecha Inicio	Fecha Final
Diagnóstico	Actualizar Instrumento de evaluación MSPI (GAP)	Oficial de Seguridad de la Información	Matriz instrumento de evaluación MSPI (GAP)	01/02/2023	20/03/2023
	Instrumento GAP PDP	Oficial de Seguridad de la Información	Diagnóstico GAP protección de datos personales	01/02/2023	20/03/2023
Planificación	Actualizar la política y el manual de seguridad de la información alineado con los	Oficial de Seguridad de la Información	Política y Manual de lineamientos de seguridad de la información	02/03/2023	20/04/2023

[5] Adaptado del Modelo de Seguridad y Privacidad de la Información - MINTIC

Fase	Actividad	Responsable	Entregable	Fecha Programación	
				Fecha Inicio	Fecha Final
	controles de la norma ISO27001:2013				
	Plan de capacitación, sensibilización y comunicación de seguridad de la información	Dirección de planeación y direccionamiento corporativo Grupo de Formación y Desarrollo Talento Humano Oficial de seguridad de la información	Plan de sensibilización	01/03/2023	31/12/2023
Operación	Plan de implementación de controles de seguridad y privacidad de la información	Oficial de Seguridad de la Información	Plan de seguridad y privacidad de la información	01/03/2023	31/12/2023
	Actualización Política General de Seguridad y Privacidad de la información	Oficial de Seguridad de la Información	Política general de seguridad y privacidad de la información	02/04/2023	02/04/2023
	Gestión de incidentes de seguridad de la información	Oficial de Seguridad de la Información	Actualizar y socializar el procedimiento de gestión de incidentes de seguridad de la información	01/03/2023	31/12/2023
	Gestionar los incidentes de seguridad de la información de acuerdo con el procedimiento definido	Oficial de Seguridad de la Información Oficina de Sistemas	Informes de los incidentes de seguridad de la información que se materializaron de manera mensual	01/03/2023	31/12/2023
	Reporte de Novedades de los boletines del Equipo de Respuesta a Incidentes de Seguridad (CSIRT) es una organización que es responsable de recibir, revisar y responder a informes y actividad sobre incidentes de seguridad.CAI VIRTUAL entre otros medios.	Oficial de Seguridad de la Información Oficina de Sistemas	Comunicación a especialistas con las recomendaciones enviadas para contención y minimización de eventos o incidentes	01/01/2023	31/12/2023
	Seguimiento a los eventos y vulnerabilidades	Oficial de Seguridad de la Información Oficina de Sistemas	Realizar seguimiento a hallazgos de eventos y vulnerabilidades	01/01/2023	31/12/2023
	Actualizar los manuales,	Oficial de Seguridad de la Información	Políticas, guías, manuales,	01/01/2023	31/12/2023

Fase	Actividad	Responsable	Entregable	Fecha Programación	
				Fecha Inicio	Fecha Final
	procedimientos, guías operacionales y demás documentos de control que estén identificados en el GAP de madurez de la entidad.		procedimientos entre otros y formalizados en compromiso.		
	Identificación de riesgos de seguridad y privacidad de la información, seguridad digital	Oficial de Seguridad de la Información	Identificación, análisis y evaluación de los riesgos de seguridad y privacidad de la información, seguridad digital en los procesos de la dirección general.	02/02/2023	31/08/2023
	Seguimiento de riesgos de seguridad y privacidad de la información, seguridad digital	Oficial de Seguridad de la Información	Seguimiento sobre los planes de tratamiento definidos sobre los riesgos de seguridad y privacidad de la información, seguridad digital en los procesos del sistema de gestión	02/02/2023	31/08/2023
	Levantamiento de activos de información de la dirección general	Oficial de Seguridad de la Información	Guía de activos de información revisada y actualizada Matriz de activos actualizados.	02/02/2023	31/08/2023
	Acompañamiento en las auditorías internas o externas	Oficial de Seguridad de la Información	Informe de hallazgos o resultados	01/03/2023	31/12/2023
	Apoyar en la definición y/o actualización de las estrategias del SENA	Oficial de Seguridad de la Información Oficina de sistemas	Documento plan DRP tecnológico aprobado y formalizado en compromiso	01/03/2023	31/12/2023
	Actualización política de protección de datos personales y el manual de protección de datos personales	Oficial de Seguridad de la Información	Actualizar la Política de PDP y el Manual de protección PDP	15/03/2023	30/06/2023
	Definición de la política de uso correo institucional	Oficial de Seguridad de la Información	Política de correo institucional	2/03/2023	30/06/2023
	Definición de la política de criptografía	Oficial de Seguridad de la Información	Política de criptografía	12/04/2023	30/06/2023
	Definición de la política de gestión con proveedores	Oficial de Seguridad de la Información	Política de gestión de proveedores	12/04/2023	30/06/2023
	Revisión, actualización e implementación de	Oficial de Seguridad de la Información	Procedimientos, formatos, BIA y	2/05/2023	30/10/2023

Dirección General
Calle 57 No. 8 - 69 Bogotá D.C. (Cundinamarca)-PBX 57 601 5461500
@SENAComunica
www.sena.edu.co

Fase	Actividad	Responsable	Entregable	Fecha Programación	
				Fecha Inicio	Fecha Final
	políticas complementarias de continuidad del negocio.		demás documentos asociados a BCP		
Evaluación de desempeño	Actualizar los indicadores en compromiso	Oficial de Seguridad de la Información	Indicadores registrados en el aplicativo compromISO	01/02/2022	31/03/2022
	Informe con la evaluación y medición de la efectividad de la implementación de los controles del MSPI	Oficial de Seguridad de la Información	Informe gestión	30/07/2023	31/11/2023
	Resultados de las auditorías internas	Oficina de Control Interno	Informe de auditoría	1/11/2023	31/12/2023
Mejoramiento continuo	Seguimiento a las acciones correctivas y oportunidades de mejora identificadas	Oficial de Seguridad de la Información	Informe trimestral de seguimiento del plan de seguridad y privacidad de la información	02/03/2023	31/12/2023
	Sensibilización de seguridad de la información, datos personales y ciberseguridad	Oficial de Seguridad de la Información	Informe trimestral	03/03/2023	31/12/2023

Fuente: Elaboración propia

6.7. **Lineamientos Generales**

Para implementar el Modelo de Seguridad y Privacidad de la información se establecen las siguientes políticas especificas:

Tabla 2. Lineamientos específicos

Política Específica	Responsable	Objetivo
Política de organización de seguridad de la información	Oficial de Seguridad de la Información	Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información en el Servicio Nacional de Aprendizaje - SENA.
Política de seguridad de la información en la gestión de proyectos	Oficial de Seguridad de la Información y gestión de proyectos	Incluir la identificación de riesgos de seguridad de la información en la gestión de los proyectos del Servicio Nacional de Aprendizaje - SENA de cualquier alcance.
Política de dispositivos móviles y trae tu propio	Oficial de Seguridad de la Información y	Establecer las medidas de seguridad frente a la confidencialidad, integridad, privacidad y disponibilidad de

Política Específica	Responsable	Objetivo
dispositivo (BYOD)	Talento Humano	los activos de información que son accedidos, modificados, generados, transmitidos y/o eliminados desde dispositivos móviles institucionales y dispositivos personales (BYOD).
Política de teletrabajo, trabajo en casa o trabajo remoto	Oficial de Seguridad de la Información y Talento Humano	Garantizar la seguridad de toda la información y los recursos gestionados cuando se realiza el teletrabajo concientizando a todos los colaboradores, funcionarios, contratistas y proveedores de la importancia de cumplir las medidas de seguridad tanto dentro como fuera de la oficina para garantizar y preservar la confidencialidad, la integridad y la disponibilidad de los activos de información que es accedida, procesada o almacenada a través de la modalidad de teletrabajo, trabajo en casa o trabajo remoto basados en los lineamientos y medidas de soporte para proteger la información.
Política de seguridad del recurso humano	Oficial de Seguridad de la Información y Contratación	Asegurar que los funcionarios, contratistas, proveedores y operadores, comprendan sus responsabilidades y roles referentes a la seguridad y Privacidad de la información antes, durante y en la terminación laboral o contractual.
Política gestión de activos	Oficial de Seguridad de la Información Líderes de los procesos y/o directivos	Definir los límites y procedimientos frente a la identificación, uso, administración y responsabilidad asociados a los activos.
Política control de acceso	Oficial de Seguridad de la Información Dirección administrativa y Financiera Seguridad Física	Establecer quién, cómo y cuándo se puede acceder a los activos del SENA y registrar dichos accesos.
Política de criptografía	Oficial de Seguridad de la Información	Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información.
Política seguridad física y del entorno	Oficial de Seguridad de la Información Dirección administrativa y Financiera Seguridad Física	Definir lineamientos para prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.
Política de seguridad en las operaciones	Oficial de Seguridad de la Información Oficina de sistemas	Definir lineamientos para establecer operaciones correctas y seguras en las instalaciones de procesamiento de la información en el SENA.
Política seguridad de las comunicaciones	Oficial de Seguridad de la Información Oficina de sistemas	Gestionar la protección de la información que transita en las redes de comunicaciones, y sus instalaciones de procesamiento de información de soporte.
Política adquisición, desarrollo seguro y mantenimiento de	Oficial de Seguridad de la Información	Establecer las condiciones y vigilar que el desarrollo y mantenimiento llevado a cabo, tanto internamente como por proveedores externos cumpla con buenas prácticas para el

Política Específica	Responsable	Objetivo
sistemas	Oficina de sistemas	desarrollo seguro, además de establecer los criterios de seguridad que deben ser considerados en todas las etapas del desarrollo.
Política relaciones con los proveedores	Oficial de Seguridad de la Información Oficina de sistemas Contratación	Definir los requisitos de seguridad y privacidad y seguridad digital de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de el Servicio Nacional de Aprendizaje - SENA.
Políticas gestión de Incidentes de seguridad de la información	Oficial de Seguridad de la Información Oficina de sistemas	Gestionar los incidentes de seguridad y privacidad de la información y seguridad digital al interior del SENA
Política aspectos de seguridad de la información de la gestión de continuidad de negocio	Oficial de Seguridad de la Información Oficina de sistemas Comunidad Sena	La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización. Se debe Asegurar la disponibilidad de instalaciones de procesamiento de información y se debe garantizar la continuidad tecnológica y operacional.
Política de cumplimiento	Oficial de Seguridad de la Información Oficina de sistemas Oficina de Control Interno	Definir los lineamientos relacionados con la seguridad y privacidad de la información y seguridad digital.

Fuente: Elaboración propia

Dirección General
Calle 57 No. 8 - 69 Bogotá D.C. (Cundinamarca)-PBX 57 601 5461500
@SENAComunica
www.sena.edu.co

7. LIDERAZGO Y COMPROMISO

Política del Sistema

El Servicio Nacional de Aprendizaje - SENA, en el marco de su misión y entendiendo la importancia de una adecuada gestión de la información, se compromete a realizar las acciones pertinentes y de carácter obligatorio para conservar la integridad, confidencialidad, disponibilidad y privacidad de sus activos de información, los cuales soportan los procesos de la entidad, estableciendo así, el Modelo de Seguridad y Privacidad de la Información - MSPI, el cual permite que la entidad pueda gestionar adecuadamente la seguridad y privacidad de sus activos de información. Lo anterior, enmarcado en el cumplimiento de los requisitos legales, regulatorios y en concordancia con la misión y visión de la entidad.

El Consejo Directivo Nacional, la Dirección General, la Secretaría General, las Direcciones, las Jefaturas, las Direcciones Regionales y las Subdirecciones de Centro del SENA se comprometen y responsabilizan con la asignación y comunicación las funciones, obligaciones y responsabilidades de todos los colaboradores en materia de seguridad y privacidad de la información, apalancando así el establecimiento, implementación, operación, seguimiento, mantenimiento y mejora continua del MSPI.

De igual manera el SENA se compromete con lo siguiente:

- El Equipo Directivo del SENA deberá asegurarse que las políticas y los objetivos del Sistema de Gestión de Seguridad de la Información y Protección de Datos Personales sean adecuados al propósito de la entidad.
- El Equipo Directivo del SENA dispondrá los recursos administrativos y financieros necesarios para alcanzar y mantener los objetivos del Sistema de Gestión de Seguridad de la Información y Protección de Datos Personales sean adecuados al propósito de la entidad.
- El Equipo Directivo del SENA deberá velar por el cumplimiento de los requisitos legales o reglamentarios y las obligaciones contractuales en materia de seguridad que soporten el funcionamiento de la entidad.
- Toda persona que tenga acceso a información institucional del SENA debe mantener en estricta confidencialidad y no deberá compartirla ni modificarla sin la debida autorización.
- Los usuarios deben acceder exclusivamente a la información a la que tienen permisos y que es necesaria para cumplir sus funciones.

- Los usuarios tienen la obligación de reportar los incidentes de seguridad de la información y protección de datos personales, de acuerdo con los procedimientos y los canales establecidos en el MSPI.
- El SENA deberá mantener un programa de sensibilización y capacitación continuo para la comunidad de la entidad en temas de seguridad de la información y protección de datos personales.
- La comunidad del SENA debe conocer, cumplir y divulgar, ésta y todas las políticas y buenas prácticas de seguridad de la información y protección de datos personales que se desprenden del MSPI.
- El SENA gestionará los riesgos de seguridad de la información y protección de datos personales acorde con la metodología de gestión de riesgos aprobada.
- Las Políticas de Seguridad de la Información y Protección de Datos Personales son de aplicación obligatoria para todos los empleados y contratistas del SENA, así como a cualquier persona que tenga acceso a la información de carácter institucional independientemente del área en la que se encuentren y cualquiera sea el nivel de las tareas que desempeñen.
- Cualquier nivel de mando en el SENA es responsable de la implementación de las Políticas de Seguridad y Protección de Datos Personales en sus áreas de responsabilidad, así como del cumplimiento de dichas políticas por parte de su equipo de trabajo.
- Los usuarios que tengan acceso a la información y a los Sistemas de Información deben cumplir con las políticas y procedimientos establecidos en el MSPI.
- Las Políticas de Seguridad y Protección de Datos Personales deberán ser revisadas al menos una vez al año en el marco del Comité Institucional de Gestión y Desempeño, con el fin de lograr la mejora continua del MSPI.

8. ROLES Y RESPONSABILIDADES DEL MODELO DEL SISTEMA DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN- MSPI

8.1 Comité Institucional de Gestión y Desempeño

El Comité Institucional de Gestión y Desempeño es la instancia donde se deben tratar los temas de privacidad, seguridad digital y de la información del Servicio Nacional de Aprendizaje - SENA, así mismo, se establece que 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, cumplimiento, mantenimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información del SENA, contemplando los recursos necesarios para que las Políticas de Seguridad y Privacidad de la Información y de Protección de Datos Personales se integre a todos los

procesos de la Entidad. Para el logro de este propósito es necesaria la participación de los diferentes actores.

Además, el Comité Institucional de Gestión y Desempeño como autoridad competente en los temas de seguridad y privacidad de la información tendrá las siguientes responsabilidades:

1. Definir y asignar las responsabilidades asociadas a la seguridad y privacidad de la información, teniendo en cuenta la segregación de funciones, separando las que se encuentren en conflicto.
2. Revisar y aprobar la política y manual de políticas de seguridad y privacidad de la información; garantizando su difusión y aplicación en la entidad.
3. Apoyar el cumplimiento de las políticas de seguridad y privacidad de la información y protección de datos personales, por parte de los colaboradores y proveedores para que las conozcan, apliquen y cumplan.
4. Acompañar y promover el desarrollo de estrategias de seguridad y privacidad como los planes de socialización, capacitación y apropiación de los temas relacionados con el MSPI.
5. Conocer los diagnósticos del nivel de implementación del MSPI en la entidad y tomar las decisiones que sean necesarias para apoyar su mejoramiento continuo.
6. Realizar revisiones periódicas del MSPI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.
7. Motivar el entendimiento, la toma de conciencia y el cumplimiento de las políticas, normas, procedimientos y estándares establecidos.

Adicionalmente, todos los funcionarios, contratistas, instructores, aprendices y terceros que tengan vínculos laborales, de formación o contractuales con la entidad, están obligados a cumplir con las políticas, procedimientos, guías, lineamientos y demás instrumentos relacionados con el MSPI, además de reportar cualquier tipo de anomalía, evento o incidente que ponga en riesgo la seguridad y privacidad de la información.