PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Diciembre 2025

Tabla de contenido

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 las Políticas de Gobierno Digital y Seguridad Digital.

El Servicio Nacional de Aprendizaje - SENA como Entidad Pública se adhiere a las iniciativas del Modelo de Seguridad y Privacidad de la Información - MSPI y demás lineamientos del gobierno nacional, por lo cual ha establecido y mejorado continuamente el Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI; el cual a través del Plan de Seguridad y Privacidad de la Información define a alto nivel las actividades a desarrollar durante la vigencia, enfocado en cubrir todos los procesos de la Entidad a nivel de la Dirección General, Regionales y centros de formación; y con ello determinar las actividades para la implementación y mejora continua que permitan alcanzar el estado de madurez deseado en materia de seguridad y privacidad de la Información. Esta estrategia se encuentra alineada a los objetivos estratégicos, la misión y visión de la Entidad con el fin de apoyar el logro y cumplimiento de los objetivos, programas y proyectos de la entidad.

Con respecto a lo anterior desde la Dirección de Planeación y Direccionamiento Corporativo y en colaboración con todas las direcciones y jefaturas, principalmente de la Oficina de Sistemas, implementa, mantiene y mejora el modelo de gestión de la seguridad de la información que permita alcanzar y mantener dentro de las diferentes áreas y colaboradores una cultura y conciencia en el acceso y uso adecuado de la información en la Entidad.

Este Plan se ha definido con base en las mejores prácticas de seguridad de los principales marcos de referencia de la materia como lo son: ISO 27001, ISO 27002, ISO 31000, ISO 27701, el Manual de Política de Gobierno Digital y del Modelo de Privacidad y Seguridad de la Información; aplicando el ciclo de mejora continua y lo establecido para la gestión de seguridad y privacidad de la información en la vigencia 2026 de manera efectiva a nivel de la Dirección General, Regionales y Centros de formación.

1. OBJETIVO GENERAL

Incrementar el nivel de madurez en seguridad de la información, privacidad y ciberseguridad del Servicio Nacional de Aprendizaje – SENA durante la vigencia 2026, fortaleciendo la gestión de riesgos, las capacidades de prevención, detección y respuesta a incidentes, y la implementación de

controles alineados con estándares, políticas y disposiciones legales vigentes, con el fin de garantizar la confidencialidad, integridad, disponibilidad, privacidad de los activos de información y la continuidad y confiabilidad de los servicios institucionales.

2. 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, ciberseguridad y protección de la información personal.
- Asegurar la protección de los activos de información de la Entidad, a través de la identificación, clasificación y/o actualización de los activos de información y sus riesgos asociados.
- Gestionar de manera oportuna los eventos e incidentes de seguridad de la información que pongan en riesgo la integridad, confidencialidad, disponibilidad y privacidad, reduciendo su impacto y propagación.
- Fortalecer la cultura, el conocimiento y las habilidades de los funcionarios y contratistas en los temas de seguridad y privacidad de la información en el SENA.
- Incrementar el nivel de madurez del Modelo de Seguridad y Privacidad de la Información en el Servicio Nacional de Aprendizaje - SENA.

3. 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, transmitida y gestionada por la entidad, sin importar el medio, formato, presentación o lugar en la cual se encuentre.

4. REFERENCIAS NORMATIVAS

El diseño e implementación del Sistema de Gestión de Seguridad y Privacidad de la Información – SGSPI del Servicio Nacional de Aprendizaje - SENA se basa en la normatividad exigida por el Ministerio de Tecnologías de la Información y Comunicaciones – MINTIC y demás entidades que regulan en la materia:

- **Ley 1266 de 2008.** “Por la cual se dictan las disposiciones generales del Habeas 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 1273 de 2009.** “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.”
- **CONPES 3701 de 2011.** Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- **Ley 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 886 de 2014**. “Por el cual se reglamenta el Registro Nacional de Bases de Datos.”
- **Decreto 103 de 2015.** “Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.”
- **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”.
- **CONPES 3854 de 2016.** Política Nacional de Seguridad Digital.
- **Decreto 1499 de 2017.** “Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión.”
- **Decreto 728 de 2017.** “Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.”
- **Decreto 1008 del 2018.** “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”.
- **CONPES 3975 DE 2019.** Política Nacional para la Transformación Digital e Inteligencia Artificial.
- **Resolución 1519 del 2020.** “Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.”
- **CONPES 3995 de 2020** - Política Nacional de Confianza y Seguridad Digital.
- **Resolución 500 de 2021.** “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".

- **Resolución 746 de 2022.** "Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021".
- **Decreto 767 de 2022.** "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".
- **NTC-ISO/IEC 27001:2022.** Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de Gestión de seguridad de la información. Requisitos.
- **Resolución 2277 de 2025.** Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.

5. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC definió el Modelo de Seguridad y Privacidad -MSPI, el cual fue facilitado a las entidades del Estado colombiano con el fin de que estos lo adopten e incrementen el nivel de madurez en los temas de seguridad y privacidad de la información. De acuerdo con lo anterior, la metodología de implementación del Plan de Seguridad y Privacidad del SENA está basado en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) y lo establecido en el MSPI y se ejecuta a través del mapa de ruta definido a continuación:

Ilustración 1 - Ciclo del Modelo de Seguridad y Privacidad de la Información (Tomado de MinTIC)

5.1 Fase de Diagnostico

Esta fase permite por medio del uso de herramientas de diagnóstico, actividades de reconocimiento y valoración de controles de seguridad de la información, identificar cual es el estado actual de la Entidad en temas de seguridad y privacidad; el resultado de este de diagnóstico permitirá establecer el nivel de madurez en cuanto a seguridad y privacidad de la información, y así definir la hoja de ruta para las actividades en las siguientes fases del modelo.

5.1.1 Estado Actual

Teniendo en cuenta la calificación de FURAG, el SENA se encuentra en un puntaje de 80.2 en la política de seguridad digital, esto refleja el esfuerzo realizado por la entidad para apoyar la implementación del SGSPI, la actualización de las políticas y manual de políticas de seguridad y privacidad de la información, esto ha permitido avanzar en la identificación de los activos de información de la Entidad, de manera que a través del análisis de riesgo se pueda clasificar y aplicar controles que permitan mejorar el nivel de riesgo de estos activos, sin embargo se requiere de mayor esfuerzo para incrementar el nivel de implementación de la política:

POLITICAS	2024	2023	VARIACIÓN
Seguridad Digital	80,2	81,5	-1,3

El nivel de implementación del MSPI permitirá al SENA establecer la estrategia a desarrollar para la que en la vigencia 2026 se prioricen las brechas a implementar y mejorar en los procesos (21 procesos) misionales, estratégicos y de apoyo de la Entidad y toda la infraestructura que los soporte. Se realizó la medición del MSPI según el instrumento actualizado por MINTIC y por primero vez se realizó a nivel de regionales y centros de formación, obteniendo los siguientes resultados:

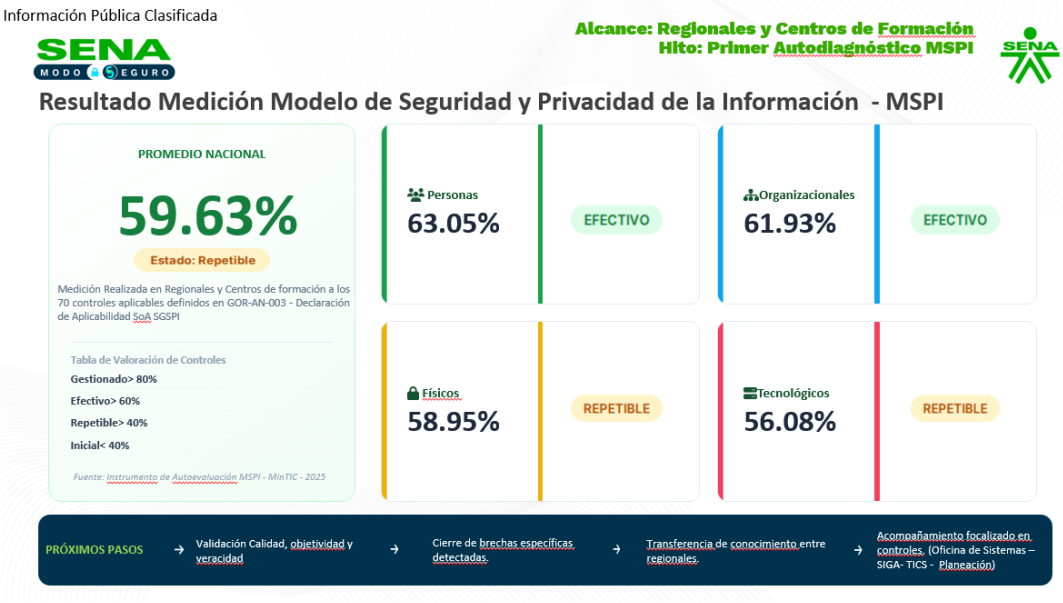

Ilustración 2 - Resultado Medición MSPI 2025 - Regionales y Centros de Formación

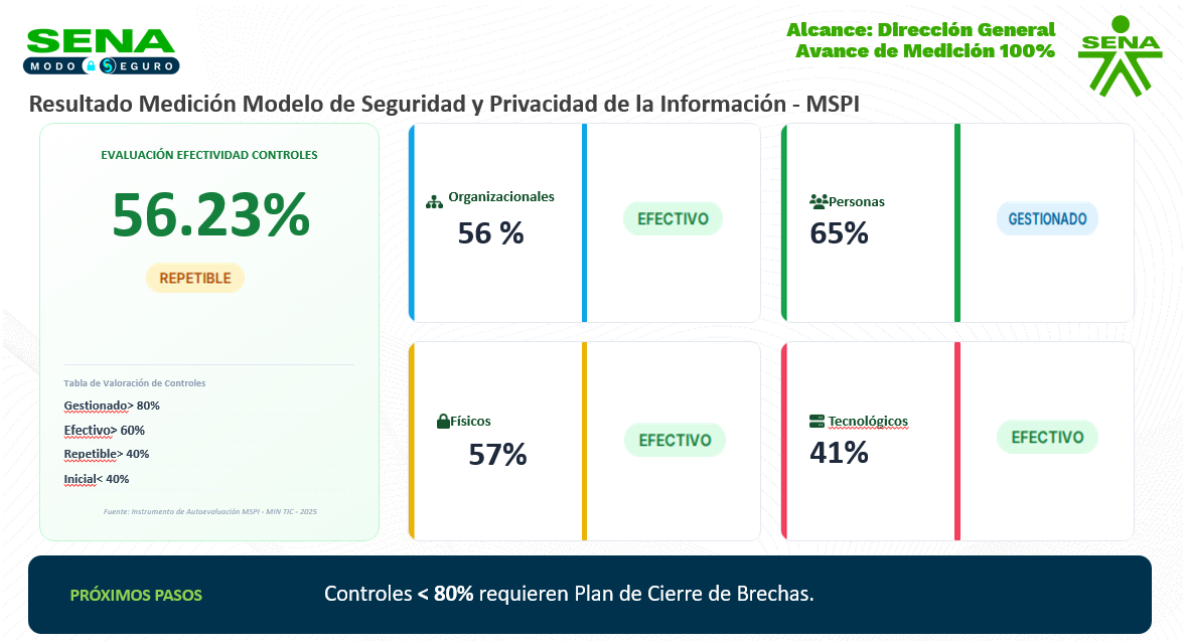

Ilustración 3 - Resultado Medición MSPI 2025 Dirección General

De igual forma se realizó en la vigencia 2025, la primera auditoría interna al Sistema de Gestión de Seguridad y Privacidad de la Información -SGSPI de manera integrada en el plan trianual de auditorías del SENA.

5.2 Fase de 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 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.

5.3 Fase de Implementación u Operación

Es necesario la implementación de la política y manual de políticas 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.

Esta fase dará paso a que el SENA lleve a cabo la implementación de los requisitos base presentados el Modelo de Seguridad y privacidad de la información – MSPI y la norma ISO/IEC 27001; de la

misma forma llegar a la implementación de los controles, que por normativa o por resultado de la identificación de riesgos deban ser implementados.

Dentro de la estrategia de la Entidad se encuentra la definición de los propósitos de seguridad y privacidad de la información, y por ende se definirán e implementarán políticas y directrices que guíen las prácticas de protección de la información en cuanto a su confidencialidad, integridad y disponibilidad. Por lo que para la vigencia 2026 estaremos centralizados en la implementación y mejora de los controles focalizado en dominio por lo que se requiere del liderazgo y apoyo de las áreas responsables de estos controles.

5.1.2 Mapa de Ruta

A continuación, se listan las actividades que el SENA planea realizar para la vigencia 2026 en temas de seguridad y privacidad de la información:

No	*Actividad*	*Fecha de inicio*	*Fecha final*	*Responsable*	*Producto o resultado esperado*
1. Activos de información					
1.1	*Diseño y puesta en funcionamiento de la herramienta para identificación y actualización de activos de información*	*Abril*	*Junio*	*Equipo Seguridad de la Información*	*Plataforma disponible*
1.2	*Socialización y acompañamiento de los lineamientos para la identificación y actualización de activos de información*	*Junio*	*Septiembre*	*Equipo Seguridad de la Información*	*Evidencias de socialización y acompañamiento*
1.3	*Identificación y Actualización de Instrumentos de gestión de la información pública*	*Junio*	*Septiembre*	*Todos los procesos SENA de la Dirección General y las 33 Regionales – acompañan Equipo Seguridad de la Información*	*Matrices de activos*
1.4	*Publicación Instrumentos de gestión de la información pública*	*Septiembre*	*Octubre*	*Dirección de Planeación y Direccionamiento Corporativo – apoyo Dirección Jurídica, Gestión Documental, Oficina de Comunicaciones*	*Registro de Activos de Información, Índice de Información Clasificada y Reservada en la página web*
1.5	*Seguimiento a la implementación de los lineamientos y estrategias para el etiquetado de los activos de tipo*	*Febrero*	*Diciembre*	*Secretaria General (Gestión Documental), Oficina de Sistemas, SIGA y Equipo Seguridad de la Información*	*Documentación con los lineamientos institucionales*

	información en medio físico y electrónico				
1.6	*Definir y socializar los lineamientos y controles sobre áreas seguras*	*Febrero*	*Marzo*	*Equipo Seguridad de la Información y Dirección Administrativa y Financiera*	*Documentos formalizados, evidencias de socialización*
2. Concienciación y Sensibilización en Seguridad y Privacidad de la Información					
2.1	*Definición del Plan de Concienciación en Seguridad y Privacidad*	*Enero*	*Febrero*	*Equipo Seguridad de la Información*	*Documento Plan de Concienciación en Seguridad y Privacidad*
2.2	*Ejecución del Plan de Capacitación y Sensibilización en Continuidad del Negocio*	*Febrero*	*Diciembre*	*Equipo Seguridad de la Información y acompañan Oficina de Comunicaciones y Grupo de formación y desarrollo del talento humano de la Secretaria General*	*Informe de ejecución Plan de Capacitación y Sensibilización en Continuidad del Negocio*
2.3	*Ejecución del Plan de Concienciación en Seguridad y Privacidad.*	*Febrero*	*Diciembre*	*Equipo Seguridad de la Información y acompañan Oficina de Comunicaciones y Grupo de formación y desarrollo del talento humano de la Secretaria General*	*Informe de ejecución Plan de Concienciación en Seguridad y Privacidad*
2.4	*Análisis de resultados del Plan de Concienciación en Seguridad y Privacidad.*	*Noviembre*	*Diciembre*	*Equipo Seguridad de la Información*	*Informe de resultados Plan de Concienciación en Seguridad y Privacidad*
3. Protección de Datos Personales					
3.1	*Seguimiento a la implementación y cumplimiento del Manual de Protección de Datos Personales.*	*Marzo*	*Noviembre*	*Dirección Jurídica con el apoyo de la Dirección de Planeación y Direccionamiento Corporativo*	*Informe de Resultado de Diagnostico*
3.2	*Ejecutar el plan de cierre de brechas de acuerdo con los resultados del diagnóstico realizado.*	*Febrero*	*Diciembre*	*Dirección Jurídica con el apoyo del equipo de seguridad de la información*	*Plan de Cierre de Brechas Informe de Resultados*
3.3	*Reporte y actualización del inventario de bases de datos de información de tipo personal del SENA en el Registro Nacional de Base de Datos (RNBD)*	*Febrero*	*Marzo*	*Dirección Jurídica con el apoyo de la Dirección de Planeación y Direccionamiento Corporativo*	*Reporte en la SIC*
3.4	*Apoyo en la implementación y desarrollo de la mesa técnica de Protección de Datos*	*Febrero*	*Diciembre*	*Dirección Jurídica con el apoyo del equipo de seguridad de la información*	*Acta de reunión, evidencias de implementación y desarrollo*

4. Implementación y mejora del Sistema de Gestión de Seguridad y Privacidad de la Información					
4.1	*Actualización y socialización del Manual de Políticas de Seguridad y Privacidad de la Información*	*Febrero*	*Mayo*	*Equipo Seguridad de la Información*	*Manual de Políticas de Seguridad de la Información formalizado y evidencias de socialización.*
4.2	*Definición del plan de cierre de brechas según la medición del MSPI por dominio*	*Enero*	*Febrero*	*Equipo Seguridad de la Información*	*Plan de Cierre de brechas por dominio*
4.3	*Definición y despliegue de la estrategia para la implementación y mejora de los controles por dominio*	*Febrero*	*Diciembre*	*Equipo Seguridad de la Información*	*Estrategia y evidencias de despliegue por dominio*
4.4	*Revisión de los controles de la norma ISO 27001:2022*	*Septiembre*	*Noviembre*	*Equipo Seguridad de la Información con el apoyo de todos los procesos*	*Herramienta de medición y autodiagnóstico del MSPI*
4.5	*Revisión por la Dirección*	*Septiembre*	*Noviembre*	*Dirección de Planeación y Direccionamiento Corporativo y Equipo Seguridad de la Información*	*Acta de Revisión por la Dirección*
4.6	*Gestionar auditoría interna al Sistema de Gestión de Seguridad de la Información*	*Abril*	*Junio*	*Grupo de Mejora Continua Dirección de Planeación y Direccionamiento Corporativo*	*Plan de Auditoria e Informe de Resultados de Auditoria*
4.7	*Acompañamiento y ejecución de las actividades de los planes de mejoramiento y planes de cierre de brechas correspondientes al SGSPI*	*Febrero*	*Diciembre*	*Todos los procesos de la entidad*	*Registro de evidencia y cierre de planes*
4.8	*Medición del nivel de implementación de la política de seguridad digital*	*Marzo*	*Mayo*	*Equipo Seguridad de la Información y Oficina de Sistemas*	*Reporte de medición*
4.9	*Ajustes, medición y seguimiento de los indicadores de seguridad de la Información*	*Febrero*	*Diciembre*	*Procesos de la Dirección General, Regionales y Centros con el apoyo del Equipo Seguridad de la Información*	*Indicadores de Seguridad y Privacidad de la información medidos*
4.10	*Seguimiento a la gestión y cierre oportuno de los incidentes y eventos de seguridad de la Información*	*Enero*	*Diciembre*	*Oficina de Sistemas con el apoyo del Grupo de Seguridad de la Información*	*Análisis del Reporte de incidentes y eventos de seguridad*

5. Continuidad del Negocio					
5.1	*Actualización del análisis de impacto al negocio – BIA para los servicios críticos de la entidad*	*Febrero*	*Marzo*	*Equipo Seguridad de la Información – con el apoyo de todos los procesos de la Dirección General*	*Documento de análisis de impacto al negocio – BIA*
5.2	*Documentar los escenarios de afectación para los servicios críticos de la entidad*	*Marzo*	*Mayo*	*Equipo Seguridad de la Información con el apoyo de todos los procesos*	*Escenarios de afectación definidos*
5.3	*Definición y socialización del Plan de Continuidad del Negocio por cada proceso priorizado*	*Marzo*	*Junio*	*Equipo Seguridad de la Información con el apoyo de los procesos priorizados*	*Plan de Continuidad del Negocio por cada proceso priorizado*
5.4	*Gestionar las pruebas a los escenarios definidos en los planes de continuidad*	*Abril*	*Noviembre*	*Procesos involucrados en los escenarios definidos*	*Informes de los resultados de las pruebas realizadas*
5.5	*Realizar el análisis de impacto al negocio – BIA para los centros de formación seleccionados*	*Julio*	*Agosto*	*Equipo Seguridad de la Información – Centros de formación seleccionados*	*Documento de análisis de impacto al negocio – BIA*
5.6	*Documentar los escenarios de afectación para los servicios críticos del centro seleccionados*	*Septiembre*	*Octubre*	*Equipo Seguridad de la Información con el apoyo de todos los procesos*	*Escenarios de afectación definidos*
5.7	*Definición y socialización del Plan de Continuidad del Negocio para los centros priorizados*	*Octubre*	*Noviembre*	*Equipo Seguridad de la Información*	*Plan de Continuidad del Negocio de los procesos seleccionados*
5.8	*Revisión y actualización de la documentación asociada a continuidad*	*Marzo*	*Diciembre*	*Equipo Seguridad de la Información*	*Documentación formalizada y socializada.*
5.9	*Acompañar la definición del Plan de Continuidad de TI, así como la planeación y ejecución de las pruebas definidas en el Plan de Continuidad de TI – DRP que impacten la continuidad del negocio*	*Febrero*	*Diciembre*	*Oficina de Sistemas con el apoyo de equipo de seguridad de información*	*Evidencias de acompañamiento*
6. Gestión de eventos e incidentes					
6.1	*Documentación y socialización de los lineamientos para la gestión de incidentes de seguridad y privacidad de la información*	*Enero*	*Abril*	*Equipo Seguridad de la Información*	*Documentos formalizados, evidencias de socialización*

6.2	*Seguimiento a la remediación de las vulnerabilidades*	*Febrero*	*Diciembre*	*Equipo de seguridad de información*	*Informes trimestrales de Seguimiento del estado y cierre de Vulnerabilidades.*
6.3	*Seguimiento a la Implementación, afinamiento y gestión de las herramientas de seguridad*	*Febrero*	*Diciembre*	*Oficina de Sistemas con el apoyo de equipo de seguridad de información*	*Informes Trimestrales de seguimiento a la implementación y afinamiento de las herramientas de seguridad*
6.4	*Realizar ejercicios y simulaciones para fortalecer el reporte y gestión de incidentes de seguridad y privacidad de la información*	*Abril*	*Octubre*	*Oficina de Sistemas con el apoyo del Equipo Seguridad de la Información*	*Informe de resultados de los ejercicios realizados.*

5.4 Evaluación de gestión

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 del SGSPI.

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.

Dado que la seguridad y privacidad de la Información es un proceso transversal a toda la Entidad, el anterior mapa de ruta establecer las acciones necesarias para implementar, gestionar, realizar seguimiento, medición y cumplimiento con respecto al objetivo de la entidad de mejorar el nivel de madurez frente al MSPI, que permitan el cumplimiento de los objetivos estratégicos de la entidad, lo anterior se mediara a través de la definición de indicadores para el SGSPI.

5.5 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.

En las actividades definidas en el mapa de ruta se contemplan varias que aportarán al mejoramiento continuo del Sistema de Gestión de Seguridad de la Información en el SENA por lo que el objetivo

de este plan es la incorporación de los temas de seguridad y privacidad de la información en todos los procesos de la entidad tanto a nivel de la Dirección General como de las regionales, centros de formación y sedes.