PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025

Diciembre 2024

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 del gobierno nacional, por lo cual ha establecido y mejorado continuamente el Sistema de Gestión de Seguridad y Privacidad de la Información; 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 y en los centros de formación; y con ello determinar el estado de madurez deseada 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 del negocio.

Con respecto a lo anterior desde la Dirección de Planeación y Direccionamiento Corporativo y en colaboración principalmente de la Oficina de Sistemas y todas las direcciones y jefaturas, el SENA 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 2025 de manera efectiva a nivel de la Dirección General y los 118 centros de formación.

1. OBJETIVO GENERAL

Definir las actividades para incrementar el nivel de madurez de seguridad y privacidad de la información del Servicio Nacional de Aprendizaje – SENA para la vigencia 2025, tomando como referencia las mejores prácticas de seguridad y privacidad como la ISO/IEC 27001 en su última versión, estrategias de Gobierno Digital, MIPG – Política de Seguridad Digital, la Política de Seguridad y Privacidad de la Información del SENA, requerimientos de la entidad y disposiciones legales vigentes; con el fin de garantizar la confidencialidad, disponibilidad, integridad y privacidad de la información de la entidad.

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 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.
- Orientar en la adopción y aplicación de la legislación relacionada con la protección de datos personales.

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 o utilizada 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."
- **Ley 1702 de 2013.** "Por la cual se crea la Agencia Nacional de Seguridad Vial y se dictan otras disposiciones."

- **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 MINTIC 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 025 de 2020.** "Por la cual se adopta la Política de Seguridad y Privacidad de la Información y se definen lineamientos para su uso, actualización y aplicación."
- **Resolución 039 de 2020.** "Por la cual se adopta la Política de Seguridad de la Información del sitio web de la Agencia Nacional de Seguridad Vial-ANSV."
- **Resolución 222 de 2020.** "Por medio de la cual adopta la Política de Protección de Datos Personales y se definen lineamientos para su uso, actualización y aplicación."
- **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 417 de 2021.** "Por la cual se constituye, integra y se establece el reglamento de funcionamiento del Comité Institucional de Gestión y Desempeño de la Agencia Nacional de Seguridad Vial y se adoptan otras disposiciones."
- **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.

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:

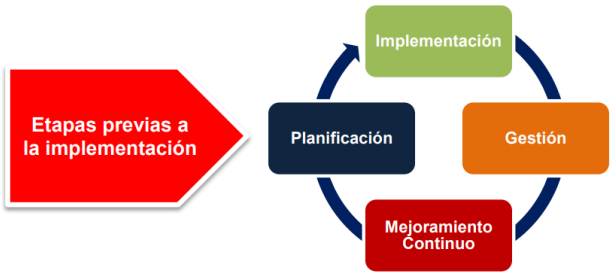

Ilustración 1 - Modelo de Operación del MSPI - tomado de MinTIC

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.

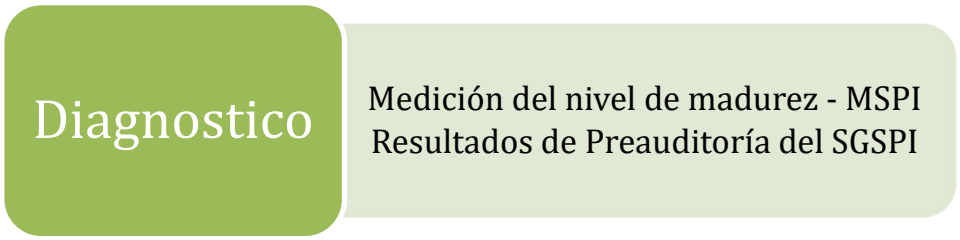

Ilustración 2 - Fase de diagnóstico

5.1.1. Estado Actual

Teniendo en cuenta la calificación de FURAG, el SENA se encuentra en un puntaje de 81.5 en la política de seguridad digital, esto se ve reflejado en 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.

El nivel de implementación del MSPI permitirá al SENA establecer la estrategia a desarrollar para la vigencia 2024 para implementar y mejorar la seguridad y privacidad de la información, para los procesos (21 procesos) misionales, estratégicos y de apoyo de la Entidad y toda la infraestructura que los soporte. El avance general en el ciclo PHVA, de acuerdo con la medición del instrumento de identificación de la línea base de seguridad, proporcionado por el Ministerio de Tecnologías de la Información y las Comunicaciones, se cuenta con un estado de implementación de la siguiente manera:

No.	Evaluación de Efectividad de controles	
	DOMINIO	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	EFECTIVO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	EFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	EFECTIVO
A.9	CONTROL DE ACCESO	EFECTIVO
A.10	CRIPTOGRAFÍA	REPETIBLE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	REPETIBLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	EFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	INICIAL
A.18	CUMPLIMIENTO	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		EFECTIVO

Con respecto a la preauditoria realizada al Sistema de Gestión de Seguridad y Privacidad de la Información por Icontec, se obtuvo los siguientes resultados:

Esto indica que la entidad debe fortalecer varios de los dominios para alcanzar por lo menos un nivel gestionado, que permita a la entidad garantizar que se están definiendo, cumpliendo y mejorando los controles de seguridad para gestionar los activos de información y los riesgos asociados a estos.

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.

Los aspectos que se tienen en cuenta para la planeación del Modelo de Seguridad y Privacidad de la información se muestran a continuación:

Ilustración 3 - Fase de planificación

5.3. Fase de Implementación u 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.

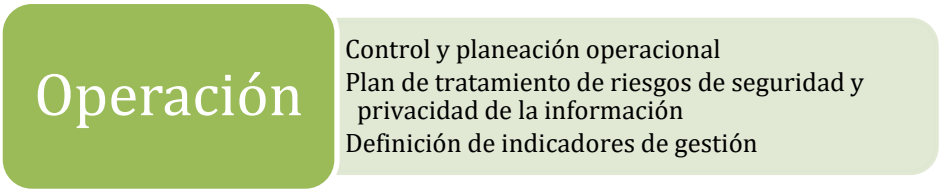

Ilustración 4 - Fase de Implementación u Operación

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.

Estas actividades permiten que el SENA empiece a tener análisis y gestión sobre los siguientes temas en el marco de seguridad: gestión de activos, gestión de comunicaciones y operaciones, gestión de recursos humanos, gestión de terceros, gestión de seguridad física, gestión de la continuidad de negocio, control de acceso lógico, cumplimiento regulatorio estrategia de seguridad en aplicaciones, estrategia de seguridad de datos y estrategia de seguridad tecnológica, entre otros.

5.3.1. Mapa de Ruta

A continuación, se listan las actividades que el SENA planea realizar para la vigencia 2025 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	Socialización y acompañamiento de los lineamientos para la identificación y actualización de activos de información	Febrero	Marzo	Equipo Seguridad de la Información	Evidencias de socialización y acompañamiento
1.2	Identificación y Actualización de Instrumentos de gestión de la información pública	Abril	Julio	Todos los procesos SENA de la Dirección General y las 33 Regionales – acompañan Equipo Seguridad de la Información	Matrices de activos
1.3	Publicación Instrumentos de gestión de la información pública	Agosto	Septiembre	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
1.4	Seguimiento a la implementación de los lineamientos y estrategias para el etiquetado de los activos de tipo información en medio físico y electrónico	Febrero	Diciembre	Secretaria General (Gestión Documental), Oficina de Sistemas, SIGA y Equipo Seguridad de la Información	Documentación con los lineamientos institucionales
1.5	Definir y socializar los lineamientos y controles sobre áreas seguras	Julio	Septiembre	Equipo Seguridad de la Información con el apoyo de la Dirección Administrativa y Financiera	Documentos formalizados
2. Riesgos de Seguridad y Privacidad de la Información					
2.1	Revisión y/o actualización de la documentación asociada a riesgos de seguridad de la información	Febrero	Abril	Equipo Seguridad de la Información, Equipo de riesgos de la Dirección de Planeación	Documentación Formalizada y Socialización

No	Actividad	Fecha de inicio	Fecha final	Responsable	Producto o resultado esperado
2.2	Identificación y Análisis de Riesgos Seguridad de la información y protección de datos de los procesos de la Dirección General	Mayo	Agosto	Todos los procesos de la Dirección General - acompañamiento de Equipo Seguridad de la Información	Matrices de riesgos
2.3	Identificación y Análisis de Riesgos Seguridad de la información y protección de datos en las Regionales	Agosto	Octubre	Todos los procesos de la Dirección General - acompañamiento de Equipo Seguridad de la Información	Matrices de riesgos
2.4	Definición de los planes de Tratamiento de Riesgos Seguridad y privacidad de la Información	Mayo	Octubre	Todos los procesos de la Dirección General - acompañamiento de Equipo Seguridad de la Información	Plan de Tratamiento de Riesgos de Seguridad de la Información
2.5	Seguimiento a la implementación de los planes de tratamiento	Noviembre	Diciembre	Equipo de Seguridad de la Información	Informe de seguimiento de los planes de tratamiento
3. Concienciación y Sensibilización en Seguridad y Privacidad de la Información					
3.1	Definición del Plan de Concienciación en Seguridad y Privacidad	Febrero	Marzo	Equipo Seguridad de la Información	Documento Plan de Concienciación en Seguridad y Privacidad
3.2	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
3.3	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
3.4	Realizar ejercicios y simulaciones para fortalecer el reporte y gestión de incidentes de	Marzo	Junio	Oficina de Sistemas con el apoyo del Equipo Seguridad de la Información	Informe de resultados de los ejercicios realizados.

No	Actividad	Fecha de inicio	Fecha final	Responsable	Producto o resultado esperado
	seguridad y privacidad de la información				
4. Protección de Datos Personales					
4.1	*Seguimiento a la implementación y cumplimiento del Manual de Protección de Datos Personales.*	*Marzo*	*Mayo*	*Dirección Jurídica con el apoyo de la Dirección de Planeación y Direccionamiento Corporativo*	*Informe de Resultado de Diagnostico*
4.2	*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*
4.3	*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*
4.4	*Apoyo en la definición de los lineamientos de propiedad intelectual*	*Abril*	*Julio*	*Dirección Jurídica con el apoyo del equipo de seguridad de la información*	*Documentación Formalizada y Socialización*
4.5	*Apoyo en la revisión de la Política, Manual de Políticas de protección de datos personales*	*Abril*	*Agosto*	*Dirección Jurídica con el apoyo de la Dirección de Planeación y Direccionamiento Corporativo*	*Documentación Formalizada y Socialización*
5. Mejora del Sistema de Gestión de Seguridad y Privacidad de la Información					
5.1	*Revisión de la Política, Manual de Políticas de Seguridad y Privacidad de la Información*	*Septiembre*	*Octubre*	*Equipo Seguridad de la Información*	*Manual y Política de Seguridad de la Información.*
5.2	*Ejecución de la estrategia para realizar la migración de la ISO 27001:2013 a la versión 2022.*	*Marzo*	*Junio*	*Equipo Seguridad de la Información con el apoyo de todos los procesos*	*Plan de Migración*

No	Actividad	Fecha de inicio	Fecha final	Responsable	Producto o resultado esperado
5.3	Revisión de los controles de la norma ISO 27001:2022	Junio	Diciembre	Equipo Seguridad de la Información con el apoyo de todos los procesos	Herramienta de medición y autodiagnóstico del MSPI
5.4	Revisión por la Dirección	Mayo	Junio	Dirección de Planeación y Direccionamiento Corporativo y Equipo Seguridad de la Información	Acta de Revisión por la Dirección
5.5	Gestionar auditoría interna al Sistema de Gestión de Seguridad de la Información	Septiembre	Octubre	Equipo Seguridad de la Información – Grupo de Mejora Continua Dirección de Planeación y Direccionamiento Corporativo	Plan de Auditoria Informe de Resultados de Auditoria
5.6	Definir los planes de mejoramiento de acuerdo con las auditorías realizadas	Febrero	Diciembre	Todos los procesos con el acompañamiento del Equipo Seguridad de la Información	Planes de Mejoramiento
5.7	Ejecución de las actividades de los planes de mejoramiento correspondientes al SGSPI	Febrero	Diciembre	Todos los procesos de la entidad	Registro de evidencia y cierre de planes
5.8	Identificación y Reporte de cumplimiento de los indicadores de seguridad de la Información	Enero	Diciembre	Equipo Seguridad de la Información y Oficina de Sistemas	Indicadores de Seguridad y Privacidad de la información
5.9	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	Reporte mensual de incidentes y eventos de seguridad
6. Continuidad del Negocio y Tecnológica					
6.1	Actualización y Formalización de la	Junio	Agosto	Equipo Seguridad de la Información – con el apoyo	Documento de análisis de impacto al negocio – BIA

No	Actividad	Fecha de inicio	Fecha final	Responsable	Producto o resultado esperado
	documentación asociada a Continuidad del Negocio			*de todos los procesos de la Dirección General*	
6.2	*Realizar el análisis de impacto al negocio – BIA para los servicios críticos de la entidad*	*Agosto*	*Octubre*	*Equipo Seguridad de la Información – con el apoyo de todos los procesos de la Dirección General*	*Documento de análisis de impacto al negocio – BIA*
6.3	*Definir los Escenarios de afectación para los servicios críticos de la entidad*	*Octubre*	*Noviembre*	*Equipo Seguridad de la Información – con el apoyo de todos los procesos*	*Riesgos de Continuidad del Negocio*
6.4	*Definición del Plan de Continuidad del Negocio*	*Noviembre*	*Diciembre*	*Equipo Seguridad de la Información*	*Plan de Continuidad del Negocio*
6.5	*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*	*Abril*	*Diciembre*	*Oficina de Sistemas con el apoyo de equipo de seguridad de información*	*Plan de Continuidad de TI - DRP*
7. Seguridad Informática					
7.1	*Seguimiento a la ejecución de análisis de vulnerabilidades, Ethical hacking, pruebas de ingeniería social, entre otros*	*Febrero*	*Diciembre*	*Oficina de Sistemas con el apoyo de equipo de seguridad de información*	*Informe de ejecución de análisis de vulnerabilidades, Ethical hacking, pruebas de ingeniería social, entre otros*
7.2	*Seguimiento a la remediación de las vulnerabilidades identificadas*	*Febrero*	*Diciembre*	*Oficina de Sistemas con el apoyo de equipo de seguridad de información*	*Informes mensuales de Seguimiento del estado y cierre de Vulnerabilidades.*
7.3	*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 Mensuales de gestión, implementación y afinamiento de las herramientas de seguridad*

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.

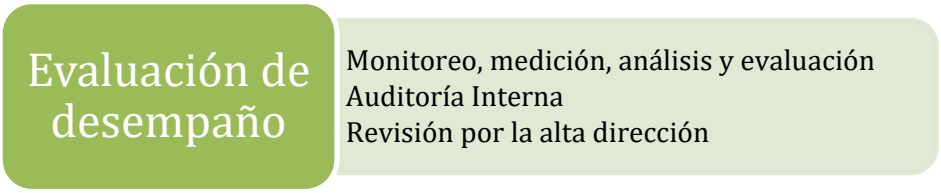

Ilustración 5 - Fase Evaluación de desempeño

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.

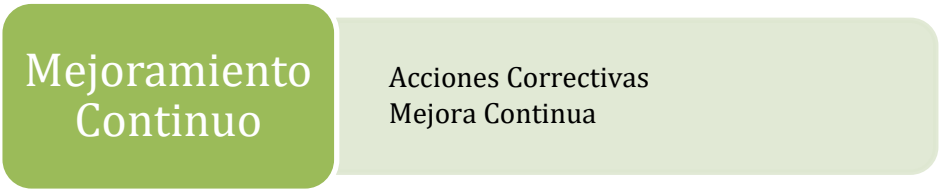

Ilustración 6 - Fase Mejora Continua

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.