PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Enero de 2024

Tabla de contenido

[INTRODUCCIÓN 3](#_Toc157013234)

[1. OBJETIVO GENERAL 3](#_Toc157013235)

[2. OBJETIVOS ESPECÍFICOS 4](#_Toc157013236)

[3. ALCANCE 4](#_Toc157013237)

[4. REFERENCIAS NORMATIVAS 4](#_Toc157013238)

[5. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 7](#_Toc157013239)

[5.1 Fase de Diagnostico 7](#_Toc157013240)

[5.1.1 Estado Actual 8](#_Toc157013241)

[5.2 Fase de Planificación 8](#_Toc157013242)

[5.3 Fase de Implementación u Operación 9](#_Toc157013243)

[5.3.1 Mapa de Ruta 10](#_Toc157013244)

[5.4 Evaluación de gestión 13](#_Toc157013245)

[5.5 Mejoramiento Continuo 14](#_Toc157013246)

Página **2** de **15**

# 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 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 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 con la Oficina de Sistemas, 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 2024 de manera efectiva a nivel de la Dirección General y los 117 centros de formación.

# 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 2024, tomando como referencia las mejores prácticas de seguridad y privacidad como la ISO/IEC 27001 en su última versión, estrategias de Gobierno Digital, MIPG, la Política de Seguridad y Privacidad de la Información y Seguridad Digital 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.

Página **3** de **15**

# 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.

# 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.

# 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”*.

Página 4de **15**

* 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”*.
* 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.
* 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*).
* NTC-ISO/IEC 27001:2022, Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de Gestión de seguridad de la información. Requisitos.
* 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.
* 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.

Página 5de **15**

* 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”.*
* 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”.
* CONPES 3854 de 2016: Política de Seguridad Digital del Estado Colombiano
* Decreto 1499 de 2017, el cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión.
* CONPES 3995 de 2020: Política Nacional De Confianza y Seguridad Digital
* Resolución 1519 de 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 materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
* 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”.

Página **6** de **15**

# 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:

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

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

## 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.

Diagnóstico

* Estado actual de la entidad
* Identificación del nivel de madurez - MSPI

Ilustración 2 Fase de diagnóstico 1

1. Adaptado del Modelo de Seguridad y Privacidad de la Información – MINTIC

Página **7** de **15**

### Estado Actual

Teniendo en cuenta la calificación de FURAG, el SENA se encuentra en un puntaje de 74,1 en seguridad digital, esto se ve reflejado en el esfuerzo realizado por la entidad para apoyar la implementación del SGSI, 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:

Tabla

Descripción generada automáticamente

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.

## 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.

Página **8** de **15**

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

**Planificación**

Contexto de la entidad

Liderazgo

Planeación

Soporte

|  |
| --- |
| * Entender a la entidad * Necesidades y expectativas de las partes interesadas * Determinar el alcance del MSPI |
| * Liderazgo y compromiso de la alta dirección * Política de seguridad * Roles de la entidad, responsabilidades y autoridad |
| * Acciones para abordar los riesgos y oportunidades * Objetivos y planes para lograrlos |
| * Recursos * Competencias * Sensibilización * Comunicación * Documentación |

## 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.

Operación

* Control y planeación operacional
* Plan de tratamiento de riesgos de seguridad y privacidad de la información
* Definición de indicadores de gestión

Ilustración 4 Fase de Implementación u Operación3

Página 9de **15**

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.

### Mapa de Ruta

A continuación, se listan las actividades que el SENA planea realizar para la vigencia 2024 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* | *Definir la documentación para la identificación y actualización de activos de información* | *Febrero* | *Marzo* | *Equipo Seguridad de la Información* | *Documentos formalizados* |
| *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 de la Oficina de Sistemas, Dirección Jurídica, Gestión Documental, Oficina de Comunicaciones* | *Registro de Activos de Información, Índice de Información Clasificada y Reservada en la página web* |
| *1.4* | *Establecer los lineamientos y estrategias para el etiquetado de los activos de tipo información en medio físico y electrónico* | *Mayo* | *Julio* | *Secretaria General (Gestión Documental), SIGA y Equipo Seguridad de la Información* | *Documentación con los lineamientos institucionales* |
| ***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* | *Abril* | *Junio* | *Equipo Seguridad de la Información* | *Documentación Formalizada y Socialización* |
| *2.2* | *Identificación y Análisis de Riesgos Seguridad de la información de los procesos de la Dirección General* | *Julio* | *Octubre* | *Todos los procesos de la Dirección General - acompañamiento de Equipo Seguridad de la Información* | *Matrices de riesgos* |
| *2.3* | *Identificación y clasificación de los riesgos asociados a gestión de los datos personales de los procesos de la Dirección General* | *Julio* | *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* | *Julio* | *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 Secretaria General Grupo de Formación y desarrollo del Talento Humano – Grupo Relaciones Laborales* | *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* |
| ***4. Protección de Datos Personales*** | | | | | |
| *4.1* | *Diagnóstico sobre el estado de cumplimiento y madurez del SENA frente a los principios y disposiciones de la Ley de protección de datos personales, sus decretos reglamentarios, la Guía y los de treinta y un (31) controles de la norma ISO 27701 para responsables del tratamiento de datos.* | *Marzo* | *Mayo* | *Dirección de Planeación y Direccionamiento Corporativo acompaña Dirección Jurídica.* | *Informe de Resultado de Diagnostico* |
| *4.2* | *Definir y ejecutar el plan de cierre de brechas de acuerdo con los resultados del diagnóstico realizado.* | *Junio* | *Diciembre* | *Dirección de Planeación y Direccionamiento* | *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)* | *Marzo* | *Marzo* | *Equipo Seguridad de la Información* | *Reporte en la SIC* |
| ***5. Sistema de Gestión de Seguridad 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* | *Definir la estrategia para realizar la migración de la ISO 27001:2013 a la versión 2022.* | *Marzo* | *Junio* | *Equipo Seguridad de la Información* | *Plan de Migración* |
| *5.3* | *Revisión de los controles de la norma ISO 27001:2022* | *Junio* | *Diciembre* | *Equipo Seguridad de la Información* | *Herramienta de medición y autodiagnóstico del MSPI semestral* |
| *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* | *Oficina de Control Interno con el apoyo del Equipo Seguridad de la Información* | *Plan Anual de Auditoria* |
| *5.6* | *Definir los planes de mejoramiento de acuerdo con las auditorías realizadas* | *Febrero* | *Diciembre* | *Todos los procesos y acompaña Equipo Seguridad de la Información* | *Planes de Mejoramiento* |
| *5.7* | *Ejecución de las actividades de los planes de mejoramiento correspondientes al SGSI* | *Febrero* | *Diciembre* | *Equipo Seguridad de la Información* | *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* | *Indicadores de Seguridad y Privacidad de la información* |
| ***6. Continuidad del Negocio*** | | | | | |
| *6.1* | *Actualización y Formalización de la documentación asociada a Continuidad del Negocio* | *Junio* | *Agosto* | *Equipo Seguridad de la Información – con el apoyo de todos los procesos de la Dirección General* | *Documento de análisis de impacto al negocio – BIA* |
| *6.2* | *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* |

## 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 SGSI.

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.

Evaluación de desempeño

* Monitoreo, medición, análisis y evaluación
* Auditoría Interna
* Revisión por la alta dirección

Ilustración 5 Fase Evaluación de desempeño4

3 Adaptado del Modelo de Seguridad y Privacidad de la Información - MINTIC

De 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 SGSI.

## 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

Mejoramiento continuo

* Acciones correctivas
* 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.

Página **14** de **14**