PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 2025

Diciembre 2024

Tabla de contenido

INTRODUCCIÓN

La seguridad y privacidad de la información en las entidades tiene como objetivo la protección de cualquier tipo de activo de información ante una serie de amenazas o brechas que atenten contra los principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad y privacidad de la información, que permitan gestionar y reducir los riesgos e impactos a los cuales está expuesta la entidad y se logre alcanzar el máximo retorno de inversión con relación al cumplimiento de la misión y visión institucionales. Por tanto, en el presente documento cuando se hable de riesgos de seguridad digital será lo mismo que decir riesgos de seguridad de la privacidad de la información digital.

El Servicio Nacional de Aprendizaje - SENA, a través de la implementación de la guía de gestión de riesgos, gestiona los riesgos de seguridad digital con el fin de reducir su probabilidad de ocurrencia y mitigar los posibles efectos de su materialización en el cumplimiento de las disposiciones legales, la protección de los activos de información y la custodia de los datos personales de los ciudadanos.

Las actividades de valoración de riesgos, en cumplimiento del Modelo Seguridad y Privacidad de la Información – MSPI del Ministerio de Tecnologías de la Información MINTIC, y la política de seguridad digital serán una herramienta para el logro de los objetivos encaminados a mantener los activos de información protegido de amenazas internas, externas y/o deliberadas.

1. OBJETIVO GENERAL

Establecer las actividades necesarias para mantener la integridad, confidencialidad, disponibilidad y privacidad de la información a través de la gestión de los riesgos de seguridad y privacidad de la información, seguridad digital, ciberseguridad y Continuidad del Servicio Nacional de Aprendizaje – SENA.

2. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad de la información aplica a todos los procesos a nivel de Dirección General, Regionales, Centros de Formación y Sedes de la entidad, donde haya recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, para el desarrollo de la misión y cumplimiento de sus objetivos estratégicos del SENA.

3. REFERENCIAS NORMATIVAS

El diseño e implementación del plan de tratamiento de riesgos de El Servicio Nacional de Aprendizaje - SENA se basa en la normatividad exigida por el Ministerio de Tecnologías de la Información y Comunicaciones - MINTIC:

- **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."

- Manual Operativo del Modelo Integrado de Planeación y Gestión - MIPG del Departamento Administrativo de la Función Pública, marzo de 2021.
- **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.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6 del Departamento Administrativo de la Función Pública, de noviembre 2022

4. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La metodología para la identificación, evaluación y gestión de riesgos de los sistemas de gestión vigentes del SENA se basa en la NTC-ISO 31000, la Guía para la administración del Riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública – DAFP, en su versión 6 - Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas del Ministerio de Tecnología de la Información y las comunicaciones y la cual se encuentra definida en Política de Administración de Riesgos - GOR-POL-008 y la Guía de Administración de Riesgos GOR-G-012, estos documentos tiene como objetivo generar un lineamiento para la gestión del riesgo del SENA, que permita la mejora continua y el cumplimiento de los objetivos institucionales mediante el tratamiento de controles fortaleciendo el desempeño de los procesos y la transparencia en la gestión Institucional y aplica para todos los procesos del SENA.

Por lo anterior de manera articulada con la Dirección de Planeación y Direccionamiento Corporativo realiza la gestión de todos los riesgos en el SENA, ya sean de gestión, corrupción, contratación, seguridad, privacidad, seguridad digital, ciberseguridad y continuidad, las actividades de identificación y análisis de los riesgos la realizan con los líderes de cada proceso como propietarios de los activos, por lo cual deben garantizar porque los custodios de las información cumplan con los controles establecidos para procurar la confidencialidad, integridad, privacidad y disponibilidad de la información institucional. El objetivo del análisis es identificar los riesgos, evaluar la pertinencia de los controles y determinar el tratamiento del riesgo que lo lleve a un nivel aceptable.

Las estrategias que lograrán la eficacia y eficiencia para la gestión de riesgos en seguridad y privacidad de la información corresponden a:

1. Establecimiento del contexto de riesgos en la Entidad donde se defina los parámetros internos y externos que se deben tomar en consideración para la identificación y valoración del riesgo. Así mismo, se debe tener en cuenta el conocimiento previo de los procesos, proyectos y en general, información de la Entidad.
2. Socializar el proceso de gestión de riesgos en seguridad de la información con la Alta Dirección y líderes de proceso para recibir el apoyo y direccionamiento a las demás partes interesadas (funcionarios, contratistas, proveedores, aprendices, entre otros).
3. Definir el medio por el cual se realizará las sesiones (virtuales o presenciales) con las partes interesadas (Alta Dirección, Líderes de proceso o a quien se delegue). Esto será sujeto a la disponibilidad del personal y recursos tecnológicos.
4. Revisar y actualizar, si aplica, la herramienta donde se registrará la información de los riesgos en Seguridad de la Información de cada proceso (Matriz de identificación y análisis de riesgos de Seguridad de la Información).
5. Socializar a los involucrados (Alta dirección, líderes de proceso, personal delegado y equipo de Seguridad de la Información) la metodología de gestión de riesgos en Seguridad y privacidad de la Información, donde se informe el objetivo, alcance, conceptos generales, herramientas y demás información relevante para el entendimiento y agilidad del ejercicio.

6. Ejecución del proceso de gestión de riesgos, es decir la identificación, clasificación, valoración y registro de los riesgos, con la respectiva revisión y aprobación de cada líder de proceso o personal que se designe.

Nota: Desde la seguridad de la información se brindan los lineamientos, directrices y acompañamiento para la gestión de riesgos en seguridad de la información de los procesos, pero es responsabilidad de cada líder de proceso o a quien se delegue, mantener actualizado la matriz de riesgos a su cargo.

7. Consolidación de la información obtenida durante el ejercicio para un posterior análisis.
8. Elaboración de un informe que contenga de manera ejecutiva los resultados de la identificación, clasificación y valoración de los riesgos en seguridad de la información.
9. Socializar con las partes interesadas (Alta dirección, líderes de proceso, personal delegado y equipo de seguridad de la información) los resultados obtenidos del proceso de gestión de riesgos en seguridad. Durante esta actividad es vital que se mencione la importancia de la gestión de riesgos como un proceso dinámico y que perdure en el tiempo, por tanto, debe ser realizado de manera periódica (al menos una vez al año) por los responsables de los riesgos o cuando se presenten cambios en: la tecnología o los procesos. Por consiguiente, el líder o responsable de los riesgos del proceso debe:
    a. Informar cuando se identifique un nuevo riesgo de Seguridad de la Información en el proceso para ser analizado y documentado, en caso de aplicar en la matriz de riesgos.
    b. Revisar y actualizar, cuando aplique, la valoración del riesgo (probabilidad e impacto).

4.1. Mapa de Ruta

A continuación, se listan las actividades que el SENA planea realizar para la vigencia 2025 para el tratamiento de los riesgos de seguridad y privacidad de la información:

#	Actividad	Fecha inicio	Fecha final	Responsable	Producto o resultado esperado
Riesgos de Seguridad y Privacidad de la Información					
1	*Revisión y/o actualización de la documentación asociada a riesgos de seguridad de la información*	*Febrero*	*Abril*	*Grupo de Mejora Continua de la Dirección de Planeación y Direccionamiento Corporativo con el apoyo del Equipo Seguridad de la Información*	*Documentación Formalizada y Socialización*
2	*Afinamiento del módulo de riesgos de seguridad y privacidad de la información en Compromiso*	*Febrero*	*Abril*	*Equipo Seguridad de la Información*	*Modulo con los requerimientos institucionales*
3	*Piloto de identificación y clasificación de riesgos de seguridad y privacidad.*	*Marzo*	*Abril*	*Equipo Seguridad de la Información*	*Resultados del piloto*
4	*Socialización de la documentación y lineamientos relacionados con la identificación y clasificación de riesgos de seguridad y privacidad de la Información.*	*Mayo*	*Junio*	*Equipo Seguridad de la Información*	*Listas de asistencia, formularios de pruebas de conocimiento.*

#	Actividad	Fecha inicio	Fecha final	Responsable	Producto o resultado esperado
5	*Identificación, documentación, análisis y valoración de Riesgos de seguridad y privacidad de la información en la herramienta institucional para los procesos de la Dirección General*	*Mayo*	*Agosto*	*Todas las áreas de la Dirección General acompañamiento de Equipo Seguridad de la Información*	*Matriz de Riesgos*
6	*Definición de planes de tratamiento para la mitigación de los riesgos*	*Mayo*	*Agosto*	*Todas las áreas de la Dirección General acompañamiento de Equipo Seguridad de la Información*	*Planes de tratamiento*
7	*Seguimiento a la ejecución de los planes de tratamiento definidos*	*Noviembre*	*Diciembre*	*Grupo de Mejora Continua de la Dirección de Planeación y Direccionamiento Corporativo con el apoyo del Equipo Seguridad de la Información*	*Informe de seguimiento de los planes de tratamiento*