PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Plan Institucional aprobado por el Comité Extraordinario Nº 2 de Gestión y Desempeño el 31 de Enero de 2023.

Enero 2023

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

TABLA DE CONTENIDO

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

1. INTRODUCCIÓN

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.

2. OBJETIVO

Definir los lineamientos que permitan gestionar los riesgos de seguridad de la información digital en el Servicio Nacional de Aprendizaje-SENA, que permita realizar el análisis, valoración, seguimiento y monitoreo permanente de los riesgos encaminados al cumplimiento de la Política de Gestión del Riesgo para el mejoramiento continuo del desempeño institucional, de tal forma que se definan y apliquen los controles de seguridad con los cuales se buscan mitigar la materialización de los riesgos de seguridad de la información digital en la entidad.

3. ALCANCE

El Plan de tratamiento de riesgos de seguridad de la información aplica a todos los procesos de El Servicio Nacional de Aprendizaje - SENA, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad digital que adopta la entidad.

4. TÉRMINOS Y DEFINICIONES

- Activo de información: en relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la entidad.

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

- Administración del riesgo: comprende el conjunto de elementos de control y sus interrelaciones, para que la institución evalúe e intervenga aquellos eventos, tanto internos como externos, que puedan afectar de manera negativa el logro de sus objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

- Amenaza: es la causa potencial de una situación de incidente y no deseada por la organización.

- Análisis de riesgos: elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad para su aceptación y manejo.

- Confidencialidad: propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

- Disponibilidad: propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

- Estimación del riesgo: proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

- Evaluación de riesgos: combinación de la probabilidad de ocurrencia de un riesgo con el impacto de su materialización, que permite determinar el grado de exposición de la entidad.

- Evento: un incidente o situación que ocurre en un lugar determinado durante un periodo de tiempo específico. Este puede ser cierto o incierto y su ocurrencia puede ser única o ser parte de una serie.

- Impacto: las consecuencias que puede ocasionar a la entidad la materialización del riesgo.

- Incidente de seguridad de la información: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones de la entidad y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

- Integridad: propiedad de la información relativa a su exactitud y completitud.

- Riesgo: efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

- Riesgo inherente: es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles. El resultado de combinar la probabilidad con el impacto permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

- Riesgo residual: el resultado de aplicar la efectividad de los controles al riesgo inherente.

- Vulnerabilidad: es aquella debilidad de un activo o grupo de activos de información, o de un control que puede ser explotada por una o más amenazas.

5. 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 527 de 1999 del Congreso de la República. Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.

- Ley 1273 de 2009 del Congreso de la República. 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.

- Ley 1581 de 2012 del Congreso de la República. Por la cual se dictan disposiciones generales para la protección de datos personales.

- 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.

- Decreto 1377 de 2013 de la Presidencia de la República. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

- Decreto 1499 de 2017 de la Presidencia de la República. Por medio de la cual se modifica el Decreto 1083 de 2015, Decreto único reglamentario de la función pública, en lo relacionado con el Sistema de Gestión establecido en el artículo de la Ley 1753 de 2015.

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

- 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.

- Manual Operativo del Modelo Integrado de Planeación y Gestión - MIPG del Departamento Administrativo de la Función Pública, marzo de 2021.

- Modelo de Seguridad y Privacidad de la Información (MSPI), Política de Gobierno Digital, Ministerio de Tecnologías de la Información y las Comunicaciones.

- NTC-ISO/IEC 27001:2013, Tecnología de la información. Técnicas de seguridad (ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements).

- Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 del Departamento Administrativo de la Función Pública.

6. TRATAMIENTO DEL RIESGO

La metodología para el tratamiento de riesgos adoptada en El Servicio Nacional de Aprendizaje - SENA es la generada por el Departamento Administrativo de la Función Pública y el Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC.

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos, estas actividades se estructuraron de la siguiente manera, siguiendo los lineamientos establecidos en la Guía de Administración del Riesgo GR-G-001 del SENA y la política de Administración del Riesgo.

ACTIVIDADES	TAREAS	RESPONSABLE	FECHAS PROGRAMACIÓN	
			FECHA INICIO	FECHA FINAL
Levantamiento de activos de información	Actualizar activos de información a nivel nacional	Oficial de Seguridad de la Información Responsable de Procesos Dinamizadores SIGA	28/02/2023	03/12/2023
Actualización lineamientos de Riesgos	Actualizar Política y Metodología de Gestión de Riesgos	Oficial de Seguridad de la Información	28/02/2023	30/30/2023
Socialización	Socializar Guía y Política de seguridad digital	Oficial de Seguridad de la Información	28/02/2023	30/30/2023

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

ACTIVIDADES	TAREAS	RESPONSABLE	FECHAS PROGRAMACIÓN	
			FECHA INICIO	FECHA FINAL
Socialización	Herramienta de Gestión de riesgos en la plataforma compromiso	Oficial de Seguridad de la Información	1-04-2023	5-05-2023
Identificación de Riesgos de Seguridad yPrivacidad de la Información	Identificación, Análisis yEvaluación de Riesgos de la plataforma compromiso de la dirección general	Oficial de Seguridad de la Información Responsables de Procesos Dinamizadores SIGA Equipos de trabajo	01/02/2023	03/12/2023
Diseño del Plan de Tratamiento de Riesgos	Diseñar del Plan de Tratamiento de Riesgos	Oficial de Seguridad de la Información Responsables de Procesos Dinamizadores SIGA Equipos de trabajo	01/02/2023	03/12/2023
Publicación Plan de Tratamiento de Riesgos	Publicación Matriz de riesgos con el plan de tratamiento para toda la dirección general	Oficial de Seguridad de la Información	14-12-2023	31-12-2023
Desarrollo Plan de Tratamiento de Riesgos	Ejecutar Plan de Tratamiento de Riesgos	Oficial de Seguridad de la Información	14-12-2023	31-12-2023
Monitoreo y Revisión	Generación presentación y reporte de indicadores	Oficial de Seguridad de la Información	01/02/2023	03/12/2023

7. DECLARACIÓN DE APLICABILIDAD

Una vez se establezca la forma en que se tratará cada riesgo sobre los activos de información (aceptar, reducir, evitar o transferir) y siguiendo con el Modelo de Seguridad y Privacidad definido por el Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC y elegidos e Auditables los controles para mitigar el riesgo se realiza el documento de declaración de aplicabilidad con las actividades necesarias para la aplicación de los controles descritos anteriormente.

8. MONITOREO Y SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración iterativa de los riesgos de seguridad de la información.

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

Los riesgos son dinámicos como la misma entidad, por tanto, podrán cambiar de forma o manera radical sin previo aviso. Por ello es necesaria una supervisión continua que detecte:

- Nuevos activos o modificaciones en el valor de los activos.
- Nuevas amenazas.
- Cambios o aparición de nuevas vulnerabilidades.
- Aumento en el número o el nivel de las consecuencias o impactos.
- Incidentes de seguridad de la información.

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad y privacidad de la información, se deberán definir esquemas de seguimiento y medición al sistema de gestión de riesgos que permitan contextualizar una toma de decisiones de manera oportuna, para cual dividimos en cuatro fases su gestión:

FASE 1: Activos de Información

- Levantamiento de Información
- Clasificación de los activos de información
- Socialización y publicación

FASE 2: Plan Seguridad y Privacidad de la Información

- Identificación de Riesgos
- Plan de Tratamiento de Riesgos
- Publicación tratamiento de Riesgos

FASE 3: Evaluación de Riesgos de Seguridad y Privacidad de la Información

- Controles según en análisis y evaluación de riesgos
- Validar riesgos mitigados en la evaluación de riesgos
- Analizar aplicabilidad de las medidas
- Priorización de las medidas
- Definir los responsables de cada uno de los riesgos
- Establecer objetivos sobre cada uno de los riesgos
- Definir las Actividades a realizar

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

FASE 4: Monitoreo de Controles de Riesgos de Seguridad y Privacidad de laInformación

- Identificación, análisis y valoración de riegos por parte de los lideres de procesos en materia de seguridad de lainformación.
- Revisión y ajustes por parte del oficial de seguridad de la información.
- Definición y plan de trabajo para los riesgos con riesgo alto o medio.

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