PROCESO
GESTIÓN ORGANIZACIONAL Y DEL RIESGO
NOMBRE DEL DOCUMENTO
POLÍTICA INTEGRAL PARA LA ADMINISTRACIÓN DE RIESGOS

Copia Controlada

Julio de 2023

Sistema Integrado de Gestión y Autocontrol

Tabla de contenido

1. INTRODUCCIÓN 4
2. OBJETIVO 4
3. ALCANCE 5
4. POLÍTICA 5
5. COMPROMISOS DE LA ALTA DIRECCIÓN 5
6. LINEAS DE DEFENSA Y NIVELES DE RESPONSABILIDAD FRENTE A LA GESTIÓN DE RIESGOS 7
7. VALORACIÓN DEL RIESGO 11
7.1 Criterios para definir el nivel de probabilidad 12
7.2 Criterios para definir el nivel de impacto 13
7.3 Lineamientos para los riesgos de corrupción 14
7.3.1 Criterios para definir el nivel de probabilidad en riesgos de corrupción 15
7.3.2 Criterios para definir el nivel de impacto en riesgos de corrupción 16
7.3.3 Análisis del impacto en riesgos de corrupción 18
7.4 Lineamientos para los riesgos de seguridad de la información 18
8. NIVELES DE SEVERIDAD DEL RIESGO 18
9. CAPACIDAD Y APETITO AL RIESGO 19
10. ESTRATÉGIAS DE TRATAMIENTO DE LOS RIESGOS 21
11. ESTRATÉGIA DE TRATAMIENTO Y MONITOREO DE LOS RIESGOS 22
12. ACCIONES A SEGUIR EN CASO DE MATERIALIZACIÓN DE LOS RIESGOS 24
13. DIVULGACIÓN DE LA POLÍTICA INTEGRAL DE ADMINISTRACIÓN DE RIESGOS 26
14. CONTROL DE CAMBIOS 27

Copia Controlada

Lista de ilustraciones

Ilustración 1 Valoración del riesgo 12
Ilustración 2 Nivel de Severidad del Riesgo 19
Ilustración 3 Capacidad y Apetito al Riesgo 20
Ilustración 4 Estrategias para combatir el riesgo 22

Copia Controlada

1. INTRODUCCIÓN

En cumplimiento con lo establecido por el Departamento Administrativo de la Función Pública (DAFP) en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas y el Modelo Integrado de Planeación y Gestión (MIPG), a continuación, se dan a conocer los elementos de la Política Integral para la Administración de Riesgos, como compromiso de la Alta Dirección del SENA.

Es importante resaltar que esta política utiliza como guía los lineamientos emitidos por el Departamento Administrativo de la Función Pública, (DAFP), Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTic) y la Secretaría de Transparencia de la Presidencia de la República correspondientes a los riesgos de gestión, seguridad de la información y corrupción respectivamente.

La Política Integral para la Gestión de Riesgos se encuentra alineada con la planificación estratégica de la Entidad y se adopta a través de Comité Institucional de Coordinación de Control Interno; para garantizar razonablemente el cumplimiento de la misión y los objetivos institucionales, mediante la gestión eficaz de los riesgos.

Esta política responde al Modelo Integrado de Planeación y Gestión (MIPG) según Decreto 1499 de 2017, dentro de sus políticas de Política de Planeación Institucional, Política de Seguimiento del Desempeño Institucional y la Política de Control Interno.

2. OBJETIVO

El objetivo de la Política Integral para la Administración del Riesgo del SENA, es formalizar el compromiso con sus grupos de valor y de interés con respecto a la administración de los riesgos, estableciendo los lineamientos y criterios que se implementaran en todos sus

Copia Controlada

procesos y niveles, atendiendo los lineamientos normativos aplicables, orientando la toma de decisiones oportunas y minimizando los efectos adversos.

Dentro de la presente política se establecen los lineamentos generales para la gestión de riesgos de la entidad, la metodología y el proceso de dicha gestión esta descrito en detalle en la Guía de Administración de Riesgos Código DE-G-001.

3. ALCANCE

La Política Integral para la Administración de los Riesgos de gestión, de corrupción y de seguridad de la información aplica para todos los procesos del modelo de operación por procesos, dependencias, niveles de la Entidad, (Dirección General, Despachos Regionales, Centros de Formación) y Procesos o actividades tercerizadas que puedan afectar la misionalidad de la entidad.

4. POLÍTICA

El Servicio Nacional de Aprendizaje - SENA, en cumplimiento a su misionalidad, se compromete con sus grupos de valor y de interés a identificar y a gestionar aquellos riesgos que impacten el cumplimiento de su misión, visión, objetivos estratégicos, prestación de sus servicios, logro de los objetivos de sus procesos y proyectos estratégicos, estableciendo medidas de control necesarios para prevenir su materialización, mitigar su impacto o aprovechar las oportunidades surgidas del contexto incluyendo los resultados de las evaluaciones llevadas a cabo por los organismos de control, todo lo anterior alineado con los requisitos legales y o normativos aplicables vigentes.

5. COMPROMISOS DE LA ALTA DIRECCIÓN

La Alta Dirección se compromete a:

Copia Controlada

a. Proporcionar los recursos necesarios para la administración del riesgo.

b. Integrar la gestión de los riesgos a sus procesos para mejorar la toma de decisiones.

c. Fortalecer el enfoque basado en riesgos para la integración de sus Sistemas de Gestión.

d. Definir la responsabilidad diferenciada basada en el modelo de líneas de defensa.

e. Definir el tratamiento a los riesgos y las oportunidades identificadas en el marco de la administración del riesgo.

f. Articular la administración de los riesgos, para que estos sean gestionados de manera unificada durante el proceso de identificación, valoración y tratamiento de los riesgos, según lo define la Guía de Administración del Riesgo del Departamento Administrativo de la Función Pública.

g. Gestionar adecuada y efectivamente los riesgos sobre los activos de información que afectan el cumplimiento de los Objetivos Estratégicos de la Entidad.

h. Fomentar la cultura del autocontrol a partir del monitoreo y seguimiento periódico de los riesgos.

i. Actualizar la política de riesgos de acuerdo con los cambios en su contexto y o normativos aplicables.

j. Asegurarse de que se establezcan medidas de intervención (controles correctivos) cuando estas apliquen como planes de continuidad, contingencia u otras acciones que permitan mitigar los impactos derivados de la materialización.

k. Promover el establecimiento de los planes de mejora continua a partir del monitoreo y seguimiento periódico de los riesgos, para asegurar la eficacia de los controles.

Copia Controlada

l. Evaluar la necesidad de actualizar la metodología para la administración de los riesgos en la Entidad, por cambios en el contexto que sean pertinentes a la gestión del riesgo y/ó normativos aplicables.

m. Asegurar que se comuniquen en la Entidad los resultados globales de la gestión del riesgo.

n. Gestionar todo los relacionado con la prevención y resolución de conflicto de intereses de acuerdo con la normatividad vigente y documentos de la entidad.

Copia Controlada

6. LINEAS DE DEFENSA Y NIVELES DE RESPONSABILIDAD FRENTE A LA GESTIÓN DE RIESGOS

De acuerdo con lo establecido en el Modelo Integrado de Planeación y Gestión MIPG y la dimensión siete de Control Interno a continuación se relacionan las líneas de defensa con sus correspondientes niveles de responsabilidad y autoridad establecidos para la administración del riesgo, proporcionando el aseguramiento razonable de la gestión para prevenir la materialización de los riesgos.

Tabla 1 Líneas de defensa y Niveles de Responsabilidad frente a la Gestión del Riesgo

LINEAS DE DEFENSA	RESPONSABLES	RESPONSABILIDADES FRENTE A LA GESTIÒN DEL RIESGO
LÍNEA ESTRATÉGICA Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a	Comité de Dirección. Comité Institucional de Gestión y Desempeño. Comité Institucional de Coordinación de Control Interno.	**El Director General y su equipo Directivo** deben determinar los lineamientos para la administración del riesgo en la Entidad. **Someter a aprobación del Director General del Sena** la Política Integral de Administración del Riesgo y hacer seguimiento, en especial a la prevención y detección del fraude,

cargo de la alta dirección y el comité institucional de coordinación de control interno.		mala conducta y conflicto de intereses. **Aprobar y revisar** los niveles de severidad y aceptación de los riesgos frente al alcance de los objetivos. **Realizar seguimiento y análisis** periódico de los riesgos institucionales. **Retroalimentar al Comité de Dirección** de los ajustes que se deben realizar frente a la gestión del riesgo. **Analizar la gestión** del riesgo y aplicación de las mejoras. **Analizar los eventos** (Materializados) y riesgos críticos. **Evaluar el estado del sistema de control interno** y aprobar las modificaciones, actualizaciones y acciones para el fortalecimiento de la gestión del riesgo.
1ra LÍNEA DE DEFENSA Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración,	Directores, Subdirectores, Líderes de proceso, programas, proyectos y en general todos los servidores públicos de la entidad.	**Identificar y gestionar** periódicamente los riesgos y oportunidades acorde a la evaluación del contexto y entorno del proceso, implementando acciones que aseguren la efectividad de los controles y o mejoras en el diseño. **Identificar y clasificar** los activos de información como base para gestionar el riesgo que permita identificar y establecer controles efectivos que garanticen la confidencialidad, integridad y disponibilidad de la información. **Realizar seguimiento y análisis** correspondiente al mapa y matriz de riesgos del proceso. **Definir las mejoras** a la gestión del riesgo del proceso.

Copia Controlada

monitoreo y acciones de mejora.		**Supervisar la ejecución de los controles y detectar las deficiencias** de estos, determinando las acciones de mejora requeridas. **Desarrollar ejercicios de seguimiento, monitoreo y revisión** para establecer la eficacia de los controles y de las acciones de tratamiento de los riesgos. **Informar a la Dirección de Planeación y Direccionamiento Corporativo** (segunda línea de defensa) sobre los riesgos materializados, los avances y evidencias de la gestión de los riesgos del proceso. **Orientar** el desarrollo de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la entidad. **Desarrollar ejercicios de Autocontrol** generando reportes al Despacho Regional a la cual pertenece incluidas las materializaciones de eventos.
2da LÍNEA DE DEFENSA Asegura que los controles y los	Director de Planeación y Direccionamiento Corporativo.	**Identificar** los cambios en el contexto interno y externo que puedan impactar el cumplimiento de los objetivos institucionales. **Asesorar a la línea estratégica** en el análisis del contexto interno y externo, para la definición de la política de riesgos y el nivel de aceptación del riesgo. **Acompañar y orientar** a los procesos sobre la metodología para la gestión de los riesgos. **Generar recomendaciones** teniendo en cuenta la metodología de administración de riesgos. **Consolidar y presentar** el mapa de riesgos institucional (riesgos de mayor

Copia Controlada

procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende.		criticidad frente al logro de los objetivos) para su análisis y desempeño ante el Comité de Dirección. **Evaluar y monitorear** la gestión global de los riesgos de la Entidad. **Evaluar el perfil de riesgos** de la Entidad y presentarlo para aprobación del Comité Institucional de Coordinación de Control Interno. **Monitorear** la gestión de riesgo y control ejecutada por la primera línea de defensa. **Consolidar los ejercicios de Autoevaluación** de las regionales generando reportes a la Oficina de Control Interno sobre el estado de gestión de los riesgos de sus procesos a nivel nacional, incluidas las materializaciones.
2da LÍNEA DE DEFENSA Asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende.	Líderes de Proceso Directores de Regionales y Subdirectores de Centros de Formación. Supervisores e interventores de contratos y proyectos, coordinadores de otros sistemas de gestión. Comité de Contratación y otros comités.	**Determinar** los riesgos, controles y tratamientos del proceso a nivel nacional que serán gestionados desde las dependencias por la primera línea de defensa. **Monitorear** la gestión de riesgo y control ejecutada por la primera línea de defensa complementando su trabajo. **Desarrollar ejercicios de Autoevaluación** generando reportes a la Dirección de Planeación y Direccionamiento Corporativo sobre el estado de gestión de los riesgos de sus procesos a nivel nacional, incluidas las materializaciones. **Identificar los riesgos propios su proceso a nivel transversal,** establecer controles, y verificar su

Copia Controlada

		adecuada implementación a nivel nacional, garantizando su conocimiento y difusión. **Garantizar la identificación e implementación de los controles** dentro de la documentación estandarizada del proceso.
3ra LÍNEA DE DEFENSA Proporciona información sobre la efectividad del Sistema de Control Interno, a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa.	Oficina de Control Interno	**Proporcionar un aseguramiento** independiente y objetivo sobre la efectividad de la gestión del riesgo y del control. **Asesorar** de manera coordinada con la Dirección de Planeación, a la primera línea de defensa en la metodología de la gestión de riesgos y controles. **Comunicar** al Comité Institucional de Control Interno posibles cambios e Impacto en la evaluación del riesgo, detectados en las auditorías. **Presentar** al comité institucional de control interno los informes de evaluación del riesgo de la Entidad. **Efectuar** seguimiento a la gestión del riesgo de corrupción, verificando la efectividad de los controles.

Copia Controlada

Fuente: Elaboración propia

GESTORES SIGA: En el SENA se considera la figura de los Gestores SIGA, quienes son las personas claves que actúan como facilitadores en la gestión de los riesgos a la primera y segunda línea de defensa.

7. VALORACIÓN DEL RIESGO

La evaluación del riesgo inherente y riesgo residual se calcula según los lineamientos descritos en la Guía de Administración de Riesgos DE-G-001.

Ilustración 1 Valoración del riesgo

Fuente: Elaboración propia

7.1 Criterios para definir el nivel de probabilidad

La probabilidad se entiende como la posibilidad de ocurrencia del riesgo. Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la **exposición al riesgo** del proceso o actividad que se esté analizando. De este modo, **la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.**

Bajo este esquema, la subjetividad que usualmente afecta este tipo de análisis se elimina, ya que se puede determinar con claridad la frecuencia con la que se lleva a cabo una actividad.

En la tabla 2 se establecen los criterios para definir el nivel de impacto.

Tabla 2 Criterios para definir el nivel de probabilidad

	Frecuencia de la Actividad	**Probabilidad**
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%

Copia Controlada

Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Departamento Administrativo de la Función Pública DAFP - Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas.

7.2 Criterios para definir el nivel de impacto

El impacto se entiende como la consecuencia económica y/o reputacional que se generaría por la materialización del riesgo. Para la definición de la tabla de criterios se definen **impactos económicos y reputacionales** como variables principales.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, los cuales tienen diferentes niveles, se debe tomar el más alto, así por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado.

Bajo este esquema se facilita el análisis para los responsables del riesgo, dado que se puede considerar información objetiva para su establecimiento, eliminando la subjetividad que usualmente puede darse en este tipo de análisis.

En la tabla 3 se establecen los criterios para definir el nivel de impacto.

Tabla 3 Criterios para definir el nivel de impacto

	Afectación Económica	**Reputacional**
Leve 20%	Afectación menor a 10 SMLMV.	El riesgo afecta la imagen de algún área de la organización.
Menor -40%	Entre 10 y 50 SMLMV.	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.

Copia Controlada

Moderado 60%	Entre 50 y 100 SMLMV.	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV.	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV.	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

Fuente: Fuente: Departamento Administrativo de la Función Pública DAFP - Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas.

7.3 Lineamientos para los riesgos de corrupción

Riesgo de corrupción: Es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

"Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos" (Conpes N° 167 de 2013). Es necesario que en la descripción del riesgo concurran los componentes de su definición, así:

ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO.

Los riesgos de corrupción se establecen sobre procesos. El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se sugiere la utilización de la

Copia Controlada

matriz de definición de riesgo de corrupción, que incorpora cada uno de los componentes de su definición.

De acuerdo con la siguiente matriz, si se marca con una X en la descripción del riesgo que aparece en cada casilla quiere decir que se trata de un riesgo de corrupción:

Tabla 4 Matriz definición de riesgo de corrupción

DESCRIPCIÓN DEL RIESGO	ACCIÓN U OMISIÓN	USO DEL PODER	DESVIAR LA GESTIÓN DE LO PÚBLICO	BENEFICIO PRIVADO
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	**X**	**X**	**X**	**X**

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5.

Copia Controlada

7.3.1 Criterios para definir el nivel de probabilidad en riesgos de corrupción

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado pero es posible que suceda.

Tabla 5 Criterios para definir el nivel de probabilidad (riesgos de corrupción)

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA

1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años
2	Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años
3	Posible	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos 2 años
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5.

7.3.2 Criterios para definir el nivel de impacto en riesgos de corrupción

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo.

Tabla 6 Criterios para calificar el impacto en Riesgos de Corrupción

No	PREGUNTA: SI EL RIESGO DE CORRUPCION SE MATERIALIZA PODRÍA…	RESPUESTA	RESPUESTA
		SI	NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector del que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de los servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de la información de la entidad?		

Copia Controlada

10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdidas de vidas humanas?		
17	¿Afectar imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		

Responder afirmativamente de **UNA a CINCO** preguntas genera un **impacto moderado.**		
Responder afirmativamente de **SEIS a ONCE** preguntas generan un **impacto mayor.**		
Responder afirmativamente de **DOCE a DIECINUEVE** preguntas genera **un impacto catastrófico.**		
Importante: Si la respuesta a la pregunta 16 es afirmativa, el riesgo se considera catastrófico. Por cada riesgo de corrupción identificado, se debe diligenciar una tabla de estas.		
MODERADO: Genera medianas consecuencias sobre la entidad.		
MAYOR: Genera altas consecuencias sobre la entidad.		
CATASTRÒFICO: Genera consecuencias desastrosas para la entidad.		

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5.

Copia Controlada

7.3.3 Análisis del impacto en riesgos de corrupción

Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles “moderado”, “mayor” y “catastrófico”, dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos.

7.4 Lineamientos para los riesgos de seguridad de la información

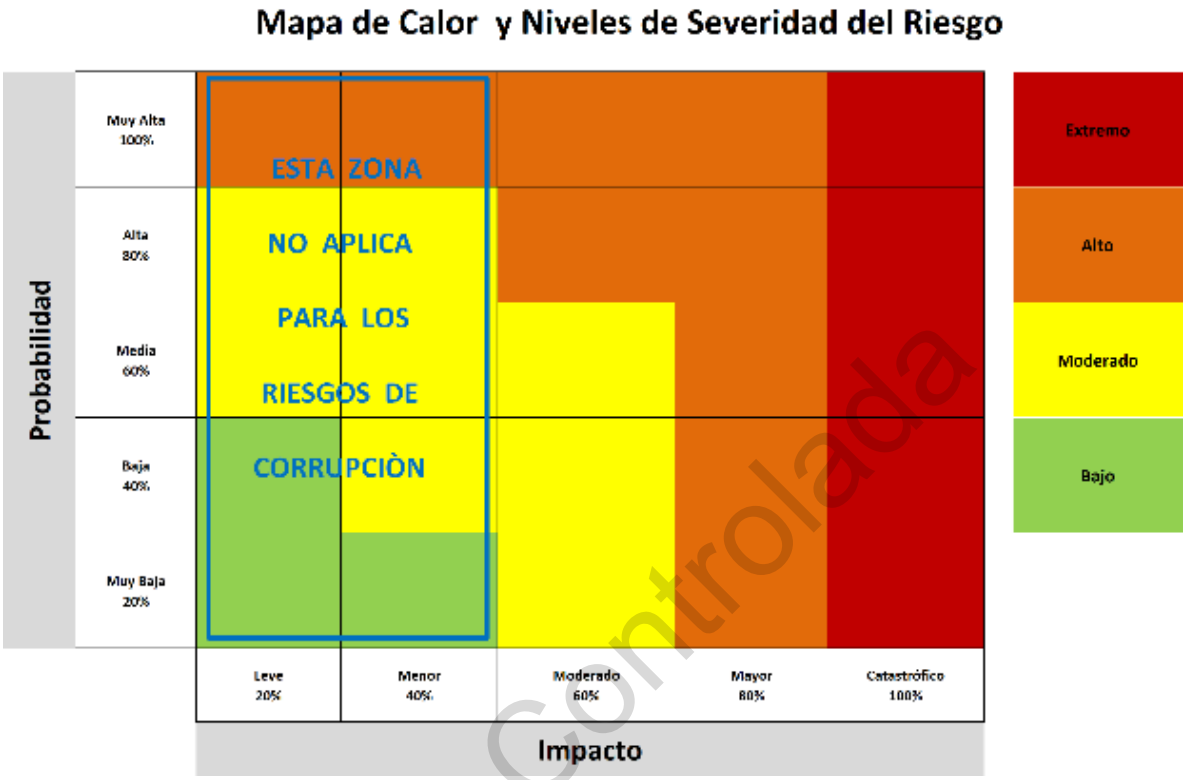
Se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI), el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales. Para mitigar y/o tratar los riesgos de seguridad de la información se empelará como mínimo los controles del Anexo A correspondientes a la norma técnica ISO/IEC 27001, con ocasión al análisis de riesgos de la entidad, mismos controles que serán documentados y caracterizados de acuerdo a las necesidades de cada proceso.

8. NIVELES DE SEVERIDAD DEL RIESGO

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial y se definen 4 zonas de severidad en el mapa de calor.

Copia Controlada

Ilustración 2 Nivel de Severidad del Riesgo



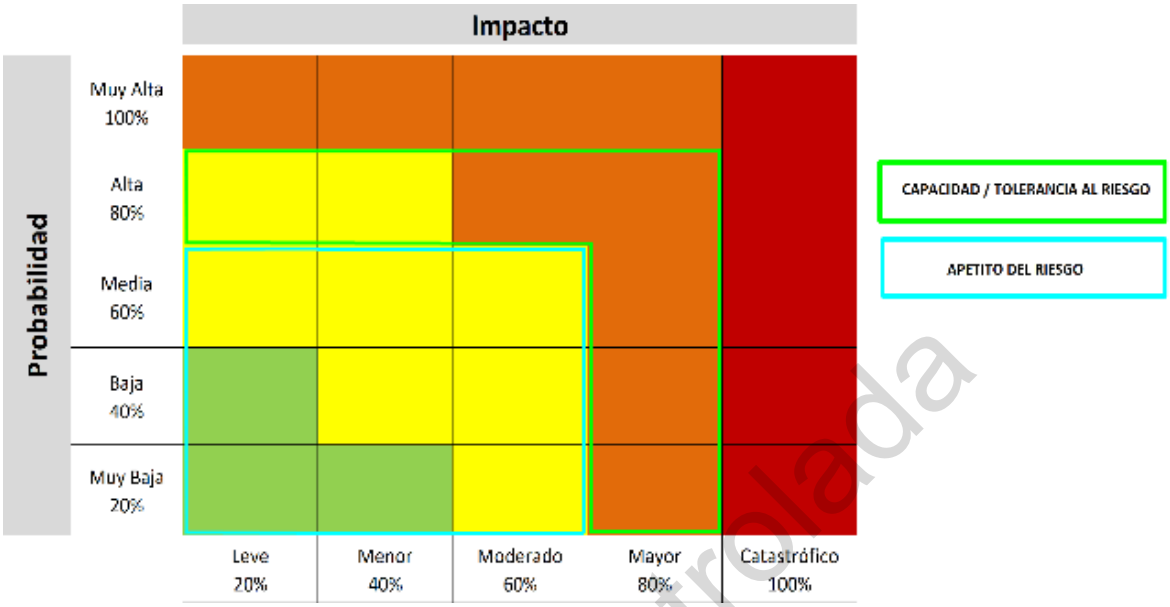
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5.

El mapa de calor permite visualizar las zonas de riesgo de acuerdo con el nivel de severidad de estos (Bajo, Moderado, Alto y Extremo) permitiendo identificar y priorizar los riesgos asociados que requieren mayor atención. Esto ayuda a la Entidad a mejorar su administración de riesgos, priorizando los esfuerzos y acciones sobre los riesgos potencialmente de mayor impacto.

9. CAPACIDAD Y APETITO AL RIESGO

Copia Controlada

Ilustración 3 Capacidad y Apetito al Riesgo



Fuente: Elaboración propia

La capacidad y apetito del riesgo están definidos según los niveles de aceptación del riesgo frente al alcance de los objetivos estratégicos de la Entidad.

El apetito del riesgo: Es valor máximo deseable que la entidad está dispuesta a aceptar y que **permitiría el logro de los objetivos institucionales** en condiciones normales de operación, se ha fijado en una zona de impacto moderado (afectación hasta 100 SMLV y ó máxima afectación de la imagen de la entidad solo con algunos usuarios de relevancia frente al logro de los objetivos) y una frecuencia menor del 60%.

La Capacidad del Riesgo: Es el valor máximo de la escala resultante de combinar la probabilidad y el impacto o el nivel máximo residual que podría soportar la entidad **antes de perder total o parcialmente la capacidad de cumplir con sus objetivos estratégicos**, estaría ubicado en el nivel de valoración de Impacto y frecuencia no mayor al 80% (equivalente a máximo 500 SMLV y ò afectación de la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, o nivel departamental o municipal).

Copia Controlada

Los riesgos que se ubiquen fuera de la Capacidad del Riesgo debe priorizarse la implementación de nuevos controles o el fortalecimiento de los existentes, ya que su materialización impactará el logro de los objetivos institucionales.

"Los conceptos de apetito de riesgo y niveles de tolerancia a riesgo solo aplican para los riesgos de Gestión y Seguridad de la información, dado que no existen niveles de permisividad a los riesgos de corrupción en el SENA".

El establecimiento de la **Tolerancia de riesgo:** valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito definido por la alta dirección y que es un valor igual o superior al apetito de riesgo y menor o igual a la capacidad del riesgo. La definición de la tolerancia es **"optativa"** para la entidad según los lineamientos establecidos por la Guía Para Administración de Riesgos y el Diseño de Controles en Entidades Públicas Versión 05 DAFP; define el nivel de riesgo que aunque la entidad tiene la capacidad de soportar también define una alarma para que se tomen medidas necesarias antes de que se llegue a la capacidad del riesgo donde se pondrá en riesgo el logro de los objetivos.

El nivel de **Tolerancia** de riesgo para la entidad se ha establecido en el mismo nivel de capacidad del riesgo, estaría ubicado en el nivel de valoración de Impacto y frecuencia no mayor al 80%.

Copia Controlada

10. ESTRATÉGIAS DE TRATAMIENTO DE LOS RIESGOS

El tratamiento de riesgos hace referencia a las estrategias para combatir el riesgo y son las decisiones que se toman frente a un determinado nivel de riesgo, pueden ser **reducir, aceptar*, y evitar**. Se analiza frente al Riesgo Residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos se procede a partir del riesgo inherente.

Ningún riesgo de corrupción será aceptado.

En la gráfica 4 se observan las tres opciones mencionadas y su relación con la necesidad de definir planes de acción dentro del respectivo mapa de riesgos.

Ilustración 4 Estrategias para combatir el riesgo

Fuente: Fuente: Departamento Administrativo de la Función Pública DAFP - Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas.

Frente al plan de acción referido para la opción de reducir, es importante mencionar que conceptualmente y de manera general se trata de herramienta de planificación empleada para la gestión y control de tareas o proyectos.

Para efectos del mapa de riesgos cuando se define la opción de reducir, se requerirá la definición de un plan de acción que requerirá: I) Responsable, II) Fecha de implementación y III) Fecha de seguimiento.

11. ESTRATÉGIA DE TRATAMIENTO Y MONITOREO DE LOS RIESGOS

Copia Controlada

En la entidad ha establecido que para los **riesgos de gestión** el nivel de aceptación se aplica a todos los riesgos que se ubiquen a nivel residual en una **zona de riesgo bajo**, el riesgo sería aceptable y asumido por la entidad.

De acuerdo con la Secretaria de Transparencia para los **riesgos de corrupción** no hay niveles de aceptación o tolerancia, por lo que siempre deben conducir a un tratamiento y **mantenerse de ser posible en un nivel moderado**.

Para los **riesgos de seguridad de la información**, sólo son tolerables los riesgos que se ubiquen a nivel residual en una **zona de riesgo bajo**.

Tabla 7 Estrategia de Tratamiento y Monitoreo del Riesgo

TIPO DE RIESGOS	ZONA DE RIESGO	ESTRATÉGIA DE TRATAMIENTO	FRECUENCIA DEL MONITOREO
Gestión	Baja	Aceptar	Cuatrimensual (Cada 4 meses)
Gestión	Moderada	Reducir - Mitigar - Transferir	Bimestral (Cada 2 meses)
Gestión	Alta y Extrema	Reducir - Mitigar - Transferir - Evitar	Mensual
Corrupción	Moderada	Reducir - Mitigar - Transferir	Bimestral (Cada 2 meses)
Corrupción	Alta y Extrema	Reducir - Mitigar - Transferir - Evitar	Mensual
Seguridad de la Información	Baja	Aceptar	Cuatrimensual (Cada 4 meses)
Seguridad de la Información	Moderada	Reducir - Mitigar - Transferir	Bimestral (Cada 2 meses)

Copia Controlada

Seguridad de la Información	Alta y Extrema	Reducir - Mitigar Transferir - Evitar	Mensual

12. ACCIONES A SEGUIR EN CASO DE MATERIALIZACIÓN DE LOS RIESGOS

En caso que se detecte la materialización, se establece las siguientes acciones a realizar de acuerdo con el tipo de riesgo.

Tabla 8 Acciones a implementar en caso de materialización del Riesgo.

RESPONSABLE	ACCIONES A IMPLEMENTAR	CORRUPCIÓN	GESTIÓN	SEGURIDAD DE LA INF.
Líder de Proceso	Sino es líder del proceso el que identificó la materialización del riesgo, se debe Informar al líder del proceso sobre el hecho encontrado inmediatamente.	X	X	X
Líder de Proceso	Informar a la Oficina de Control Interno Disciplinario sobre el hecho encontrado, con el fin de determinar las acciones a tomar.	X		
Líder de Proceso	Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante la instancia de control correspondiente.	X	Cuando aplique	Cuando aplique
Líder de Proceso	Informar al Proceso de Direccionamiento Estratégico por escrito (Correo	X	X	X

Copia Controlada

	electrónico) – Gestión de Riesgos sobre el hecho encontrado: máximo tres días hábiles después de la materialización.			
Líder de Proceso	Efectuar el análisis de causas y determinar las acciones correctivas y de mejora necesarias y documentarlas en el plan de mejoramiento.	X	X	X
Líder de Proceso	Establecer el plan de tratamiento para establecer nuevos controles o fortalecer los existentes con el objetivo de evitar una nueva materialización.	X	X	X
Líder de Proceso	Actualizar Mapa de Riesgos: Registrar la materialización del riesgo en el módulo correspondiente y volver a realizar el análisis, **valoración** y tratamiento del riesgo.	X	X	X
Líder de Proceso	Informar al CISO del Proceso de Direccionamiento Estratégico sobre el hallazgo y las acciones tomadas, esto con el fin de que este realice el seguimiento al cierre de las brechas detectadas por la materialización del riesgo de seguridad digital.			X
Oficina de Control Interno Disciplinario	Iniciar el debido proceso disciplinario de acuerdo a procedimiento aplicable.	X	Cuando aplique	Cuando aplique

Copia Controlada

Oficina de Control Interno de Gestión	Verificar que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente.	X	X	X
Dirección de Planeación y Direccionamiento Estratégico	Se deben informar los riesgos materializados en los diferentes procesos al Comité Institucional de Control Interno para establecer acciones y medidas adicionales a tomar.	X	X	X
Dirección de Planeación y Direccionamiento Estratégico	Verificar que se establezcan las acciones de mejora con el líder del proceso.	X	X	X
Dirección de Planeación y Direccionamiento Estratégico	Verificar la actualización de los mapas de riesgos.	X	X	X

Copia Controlada

13. DIVULGACIÓN DE LA POLÍTICA INTEGRAL DE ADMINISTRACIÓN DE RIESGOS

La divulgación de la Política Integral de Administración del Riesgo de la Entidad, estará a cargo de la Dirección de Planeación y Direccionamiento Corporativo y será publicada en la plataforma Compromiso con el fin asegurar la disponibilidad y consulta de todos los servidores de la Entidad. Así mismo, se publicará en el link de transparencia de la página WEB del SENA para que este disponible a las partes interesadas y grupos de valor.

Se realizarán un evento de divulgación y socialización a nivel nacional de la Política de Administración de Riesgos. Para complementar lo anterior, se realizará mesas de trabajo en las cuales se reforzará los lineamientos de la gestión del riesgo con Regionales, Centros de Formación y los procesos de la entidad.

14. CONTROL DE CAMBIOS

VERSION	FECHA DE ENTRADA EN VIGENTE	NATURALEZA DEL CAMBIO
1	Julio 2023	De acuerdo con la aprobación de la actualización del mapa de procesos por el Comité Institucional de Gestión y Desempeño, se hace actualización de código e imagen institucional, reemplazando el documento GR-POL-001 V 02 por GOR-POL-008 V 01.

Copia Controlada