

 <p>FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA</p> <p>ADMINISTRACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN</p>	<p>SISTEMA INTEGRADO DE GESTIÓN</p> <p>POLÍTICA PARA LA ADMINISTRACIÓN DEL RIESGO DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL</p>		 <p>La salud es de todos</p> <p>Minsalud</p>
<p>VERSIÓN: 1.0</p>	<p>CÓDIGO: ESESDIGPL01</p>	<p>FECHA ACTUALIZACIÓN: 12 DE JULIO 2019</p>	<p>PAGINA 1 DE 20</p>



POLÍTICA PARA LA ADMINISTRACIÓN DEL RIESGO DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL DEL FPS-FNC

Fecha de Vigencia: Junio 2019

CONTROL DE CAMBIOS			
Versión	Fecha y acto administrativo de aprobación	Cambio	Nombre del solicitante
1.0	<i>Resolucion 1621 12/07/2019</i>	DOCUMENTO NUEVO	María Yaneth Farfán C.

CONTROL DE DOCUMENTOS			
Elaborado por: Carlos Habib Olivella	Cargo: Profesional OPS	Fecha: 10-06-2019	Firma: <i>Carlos Habib Olivella</i>
Revisado Técnicamente en OPS: Martha Liliana García Leiva	Cargo: Profesional de la Oficina Asesora de Planeación y Sistemas	Fecha:	Firma: <i>Martha Liliana García Leiva</i>
Aprobado Mediante Acta No : 010 Acto Administrativo: <i>Resolucion 1621</i> Fecha: <i>12/07/2019</i>			

 <p>FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA</p> <p>ADMINISTRACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN</p>	<p align="center">SISTEMA INTEGRADO DE GESTIÓN</p> <p align="center">POLÍTICA PARA LA ADMINISTRACIÓN DEL RIESGO DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL</p>		 <p>La salud es de todos</p> <p>Minsalud</p>
<p>VERSIÓN: 1.0</p>	<p>CÓDIGO: ESESDIGPL01</p>	<p>FECHA ACTUALIZACIÓN: 12 DE JULIO 2019</p>	<p>PAGINA 3 DE 20</p>

CONTENIDO

1. OBJETIVO GENERAL.....	4
1.1 OBJETIVOS ESPECIFICOS.....	4
2. ALCANCE.....	5
3. PRINCIPIOS DE LA GESTION DEL RIESGO.....	5
4. NORMATIVIDAD APLICABLE.....	6
5. TERMINOS Y DEFINICIONES.....	7
6. POLITICA DE LA ADMINISTRACION DEL RIESGO.....	8
6.1 CICLO DE GESTION DEL RIESGO.....	9
6.2 NIVELES DE ACEPTACION DEL RIESGO.....	12
6.3 NIVELES PARA CALIFICAR EL IMPACTO.....	13
6.4 NIVELES DE AUTORIDAD Y RESPONSABILIDAD.....	14
6.5 TRATAMIENTO DEL RIESGO.....	18
6.6 GESTION DE ACCIONES CORRECTIVAS Y PLANES DE TRATAMIENTO DEL RIESGO.....	20

 <p>FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA</p> <p>ADMINISTRACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN</p>	<p>SISTEMA INTEGRADO DE GESTIÓN</p> <p>POLÍTICA PARA LA ADMINISTRACIÓN DEL RIESGO DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL</p>		 <p>La salud es de todos</p> <p>Minsalud</p>
<p>VERSIÓN: 1.0</p>	<p>CÓDIGO: ESESDIGPL01</p>	<p>FECHA ACTUALIZACIÓN: 12 DE JULIO 2019</p>	<p>PAGINA 4 DE 20</p>

1. OBJETIVO GENERAL

Establecer en el **Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia**, mediante la política para la administración del riesgo, la búsqueda de manera clara y formal con respecto a los lineamientos y metodologías que permita a todos los procesos la identificación, análisis, valoración, monitoreo, revisión y seguimiento de los riesgos, cuya finalidad sea dar un tratamiento adecuado, buscando mitigar y/o eliminar su materialización a través de la implementación de controles y acciones preventivas, y de esta manera contribuir al logro y cumplimiento de la misión y objetivos institucionales.

1.1 OBJETIVOS ESPECIFICOS

- a) Identificar los factores de riesgo al que está sometido el Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia, con el fin establecer estrategias, controles, acciones preventivas y procedimientos encaminados a su mitigación, con el objeto de garantizar el cumplimiento de la Misión y Objetivos Estratégicos de la entidad.
- b) Fijar las escalas de valoración para la probabilidad de ocurrencia y el impacto de cada factor de riesgo identificado.
- c) Administrar los riesgos identificados en los catorce (14) procesos conforme a los objetivos estratégicos del Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia, adoptando acciones que permitan el control y la mitigación de los mismos estableciendo lineamientos para la gestión de los riesgos a un nivel aceptable.
- d) Fijar las reglas para la identificación de las actividades de control que minimicen la ocurrencia e impacto de los factores de riesgo.
- e) Realizar los componentes fundamentales para el seguimiento y evaluación de las acciones y controles preventivos y detectivos implementadas en la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital en el formato macro consolidador del mapa institucional de riesgos y oportunidades ASIF11 Versión 5 adoptada del Ministerio de Salud y Protección Social, con el propósito de determinar la efectividad de los controles.
- f) Establecer el mecanismo de periodicidad para la difusión y apropiación de la política de riesgos por parte del Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia.

El desarrollo de estos objetivos se rige de acuerdo a los “Procedimiento de Administración de Riesgos”, que tienen como intención facilitar el cumplimiento de la misión y objetivos estratégicos del Fondo de Pasivo social de Ferrocarriles Nacionales de Colombia a través de la prevención y administración de los riesgos, por ende

 FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN	SISTEMA INTEGRADO DE GESTIÓN		 La salud es de todos Minsalud
	POLÍTICA PARA LA ADMINISTRACIÓN DEL RIESGO DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL		
VERSIÓN: 1.0	CÓDIGO: ESESDIGPL01	FECHA ACTUALIZACIÓN: 12 DE JULIO 2019	PAGINA 5 DE 20

contar con una metodología que permita el levantamiento de los diferentes riesgos establecidos en los procesos de la entidad, que son significativos e influyen para la mejora continua del FPS-FNC; así como la metodología para determinar el plan de contingencia a seguir en caso de que se materialicen los riesgos.

2 ALCANCE

La política para la administración del Riesgo en el Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia aplica a todos los procesos de la Entidad que operan a nivel nacional donde el Fondo tiene puntos de atención de servicio, con el fin de garantizar un adecuado conocimiento y control de los riesgos en todos los niveles organizacionales.

Los responsables de realizar la administración de los riesgos, son los líderes de los procesos, con sus respectivos equipos de trabajo, quienes deben propiciar escenarios de trabajo en donde se generen las acciones que permitan el tratamiento adecuado de los riesgos y se logre la mitigar la probabilidad de ocurrencia. De igual manera se indica que la administración del riesgo es un proceso transversal a todas las actividades del Fondo de pasivo Social de Ferrocarriles Nacionales de Colombia, incluyendo a todos los funcionarios. Con base en lo anterior se establece que la gestión de los riesgos en la entidad aplica a la totalidad de los procesos vigentes.

3 PRINCIPIOS DE LA GESTION DEL RIESGO

- Crear valor.
- Estar integrada en los procesos de la entidad.
- Estar presente en el proceso de toma de decisiones.
- Tratar explícitamente la incertidumbre.
- Ser sistemática y estructurada.
- Se basa en la mejor información de la que se dispone.
- Se adapta a circunstancias locales y específicas.
- Valorar los factores humanos y culturales.
- Ser transparente e inclusiva.
- Ser dinámica, recurrente y sensible al cambio.
- Facilitar la mejora continua de la entidad.

 FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN	SISTEMA INTEGRADO DE GESTIÓN		 La salud es de todos Minsalud
	POLÍTICA PARA LA ADMINISTRACIÓN DEL RIESGO DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL		
VERSIÓN: 1.0	CÓDIGO: ESESDIGPL01	FECHA ACTUALIZACIÓN: 12 DE JULIO 2019	PAGINA 6 DE 20

4 NORMATIVIDAD APLICABLE

Constitución Política 1991, Adopta los principios de la función administrativa y elimina el control fiscal previo y obligatoriedad para todas las entidades estatales de contar con el control interno.

Ley 87 de 1993, Crea el Sistema Institucional de Control Interno y dota a la administración de un marco para el control de las actividades estatales, directamente por las mismas autoridades.

Ley 489 de 1998, Fortalece el Control Interno, con la creación del Sistema Nacional de Control Interno.

Ley 1753 de 2015, Integra en un solo Sistema de Gestión, los Sistemas de Gestión de la Calidad (Ley 872 de 2003) y de Desarrollo Administrativo (Ley 489 de 1998) articulado con los Sistemas Nacional e Institucional de Control Interno (Ley 87 de 1993 y en los artículos 27 al 29 de la Ley 489 de 1998).

Ley 1474 2011, Dicta normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública y ordena que las entidades del orden nacional, departamental y municipal deberán elaborar anualmente una estrategia de lucha contra la corrupción y de atención al ciudadano. Dicha estrategia contemplará, entre otras cosas, el mapa de riesgos de corrupción en la respectiva entidad, las medidas concretas para mitigar esos riesgos, las estrategias anti trámites y los mecanismos para mejorar la atención al ciudadano.

Ley 1712 2014, Crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y entre otras disposiciones, ordena publicar el Plan Anticorrupción y de Atención al Ciudadano.

Decreto 2593 del 2000 Por el cual se dictan normas sobre el Sistema Nacional de Control Interno de las Entidades y Organismos de la Administración Pública del orden nacional y territorial y se dictan otras disposiciones. (Modificado parcialmente por el Decreto 2593 del 2000 y por el Art. 8 de la ley 1474 de 2011.

Decreto 1537 de 2001 Por el cual se reglamenta parcialmente la Ley 87 de 1993 en cuanto a elementos técnicos y administrativos que fortalezcan el sistema de control interno de las entidades y organismos del Estado. El párrafo del Artículo 4 señala los objetivos del sistema de control interno, define y aplica medidas para prevenir los riesgos, detectar y corregir las desviaciones, y en su Artículo 3 establece el rol que deben desempeñar las oficinas de control interno, que se enmarca en cinco tópicos valoración de riesgos. Así mismo establece en su Artículo 4 la administración de riesgos, como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas.

Decreto 1083 de 2015, Determina que las entidades públicas establecerán y aplicarán políticas de administración del riesgo, como parte integral del fortalecimiento de los sistemas de control interno. Para tal efecto, la identificación y análisis del riesgo debe ser un proceso permanente e interactivo entre la administración y las unidades de control interno o quien haga sus veces, evaluando aspectos, tanto internos como externos, que pueden llegar a representar amenaza para la consecución de los objetivos organizacionales, con miras a establecer acciones efectivas, representadas en actividades de control. Título 21 Sistema de Control Interno. Cap. 5 Art. 2.2.21.5.4 Administración de riesgos.

Decreto 1499 2017, Articula el Sistema de Gestión en el marco del Modelo Integrado de Planeación y Gestión – MIPG, a través de los mecanismos de control y verificación que permiten el cumplimiento de los

 <p>FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA</p> <p>ADMINISTRACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN</p>	<p>SISTEMA INTEGRADO DE GESTIÓN</p> <p>POLÍTICA PARA LA ADMINISTRACIÓN DEL RIESGO DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL</p>		 <p>La salud es de todos Minsalud</p>
<p>VERSIÓN: 1.0</p>	<p>CÓDIGO: ESDSDIGPL01</p>	<p>FECHA ACTUALIZACIÓN: 12 DE JULIO 2019</p>	<p>PAGINA 7 DE 20</p>

objetivos y el logro de resultados de las entidades. Actualiza el Modelo Estándar de Control Interno para el Estado Colombiano – MECI a través del Manual Operativo del Modelo Integrado de Planeación y Gestión – MIPG (correspondiendo a la 7° Dimensión de MIPG).

Directiva presidencial 09 de 1999 Lineamientos para la implementación de la política de lucha contra la corrupción.

Estándares de referencia

Norma ISO 31.000 2018, Norma internacional que proporciona principios y directivas eficaces para el tratamiento y la gestión de riesgos.

COSO ERM 2017, Marco Integrado para la Administración de Riesgos Empresariales

ISO/IEC 27001:2013, Norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.

Norma Técnica Colombiana **NTC-ISO 27001:2013** Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos

5 TERMINOS Y DEFINICIONES

- **Administración de Riesgos:** Un proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación.
- **Activo:** en el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- **Amenazas:** situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Apetito al riesgo:** magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.
- **Activo de información:** Se refiere a cualquier información o elemento relacionado con su tratamiento. ISO 27001:2005.
- **Análisis de Riesgo:** Elemento de control que permite establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente).
- **Confidencialidad:** propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

 <p>FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA</p> <p>ADMINISTRACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN</p>	<p align="center">SISTEMA INTEGRADO DE GESTIÓN</p> <p align="center">POLÍTICA PARA LA ADMINISTRACIÓN DEL RIESGO DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL</p>		 <p>La salud es de todos Minsalud</p>
<p>VERSIÓN: 1.0</p>	<p>CÓDIGO: ESESDIGPL01</p>	<p>FECHA ACTUALIZACIÓN: 12 DE JULIO 2019</p>	<p>PAGINA 8 DE 20</p>

- **Control:** medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).
- **Control Correctivo:** Este no prevé que un evento suceda, pero permiten enfrentar la situación una vez se ha presentado.
- **Control Preventivo:** Evitan que un evento suceda.
- **Calificación del Riesgo:** Es la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo.
- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Consecuencia:** los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **Corrupción:** “Uso del poder para desviar la gestión de lo público hacia el beneficio privado. CONPES # 167 del 9 de diciembre de 2013.
- **Evaluación del Riesgo:** Proceso utilizado que permite comparar los resultados de la calificación del riesgo, con los criterios definidos para establecer el grado de exposición de la entidad al mismo.
- **Evento:** Incidente o situación que ocurre en un lugar determinado durante un período determinado y éste puede ser cierto o incierto y su ocurrencia puede ser única o parte de una serie.
- **Factibilidad:** Se definen como 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 se dé.
- **Frecuencia:** Es 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.
- **Gestión del riesgo:** proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
- **Gestión del Riesgo de Corrupción:** Es el conjunto de “Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Identificación del Riesgo:** En esta etapa se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas.
- **Impacto:** Consecuencias que puede ocasionar a la organización la materialización del riesgo.

 <p>FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA</p> <p>ADMINISTRACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN</p>	<p>SISTEMA INTEGRADO DE GESTIÓN</p> <p>POLÍTICA PARA LA ADMINISTRACIÓN DEL RIESGO DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL</p>		 <p>La salud es de todos</p> <p>Minsalud</p>
<p>VERSIÓN: 1.0</p>	<p>CÓDIGO: ESESDIGPL01</p>	<p>FECHA ACTUALIZACIÓN: 12 DE JULIO 2019</p>	<p>PAGINA 9 DE 20</p>

- **Mapa de riesgos:** documento con la información resultante de la gestión del riesgo.
- **MECI:** Modelo Estándar de Control Interno que tiene como fin servir de control de controles para que las entidades del Estado logren cumplir con sus objetivos institucionales en el marco legal aplicable a ellas.
- **Monitorear:** Seguimiento a las acciones establecidas en los mapas de riesgo, evaluando la eficacia de su implementación.
- **Política de Administración del Riesgo:** Lineamiento y medidas adoptadas por la Alta Dirección para la adecuada gestión del riesgo.
- **Plan Anticorrupción y de Atención al Ciudadano:** Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.
- **Probabilidad:** Posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de frecuencia, si se ha materializado, o de factibilidad teniendo en cuenta la presencia de factores internos y externos que puedan propiciar el riesgo, aunque este no se haya materializado.
- **Riesgo:** Es la posibilidad de que suceda algún evento que tendrá un impacto negativo sobre los objetivos.
- **Riesgo de gestión:** posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- **Riesgo inherente:** es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
- **Riesgo residual:** Nivel de riesgo que permanece luego de tomar medidas de tratamiento del riesgo.
- **Riesgo de corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgo de seguridad digital:** combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
- **Riesgo de seguridad de la información:** Es el potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

 <p>FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA</p> <p>ADMINISTRACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN</p>	<p>SISTEMA INTEGRADO DE GESTIÓN</p> <p>POLÍTICA PARA LA ADMINISTRACIÓN DEL RIESGO DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL</p>		 <p>La salud es de todos Minsalud</p>
<p>VERSIÓN: 1.0</p>	<p>CÓDIGO: ESDSDIGPL01</p>	<p>FECHA ACTUALIZACIÓN: 12 DE JULIO 2019</p>	<p>PAGINA 10 DE 20</p>

- **Tolerancia al riesgo:** son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

Fuente: DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PUBLICA. (2018). Guía para la administración del riesgo y el diseño de controles en entidades públicas Riesgos de gestión, corrupción y seguridad digital versión 4. Bogotá D.C.

6 POLITICA DE LA ADMINISTRACION DEL RIESGO

El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia FPS-FNC, se compromete a controlar y mitigar los riesgos que al materializarse puedan impedir el cumplimiento de los objetivos institucionales, mediante una administración efectiva de los mismos, implementando las herramientas establecidas y las estrategias de gestión del riesgo definidas según las necesidades de la entidad, con la activa participación de la alta dirección, de los líderes de proceso, los coordinadores de Grupos Internos de Trabajo, con el Grupo de Apoyo Interdisciplinario creado para la implementación del MIPG y mejoramiento del Sistema de Control interno.

Las líneas de acción que se determinan para actuar frente a la administración del riesgo son:

Línea de acción para la administración del riesgo de gestión, de corrupción y de seguridad de la información.

Para la adecuada administración de los riesgos se establece:

- Implementar estrategias adecuadas y eficaces que asegure el ciclo de la administración del riesgo de mayor impacto para la entidad, desde la identificación, hasta el tratamiento después de controles.
- Fortalecer la efectividad de los controles y la creación de nuevos según la necesidad.
- Promover la cultura del pensamiento basado en riesgo dentro de la entidad.
- Publicar y dar a conocer el ciclo para la administración del riesgo, Niveles de Aceptación del Riesgo, Niveles para calificar el impacto y niveles de autoridad y responsabilidad frente al riesgo, que se estableció a nivel institucional.

6.1 CICLO DE GESTION DEL RIESGO

El desarrollo de los pasos establecidos para la metodología de la administración del riesgo se deberá alinear a las especificaciones técnicas establecidas en la **GUÍA POLÍTICA PARA LA ADMINISTRACIÓN DEL RIESGO DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL** ESDSDIGGS02, así como en el procedimiento ADMINISTRACIÓN DEL RIESGO PEMYMOPSPT06. Los pasos generales que se aplicaran al interior del FPS-FNC, se establecen en la siguiente ilustración y está basada en la metodología establecida por el Departamento Administrativo de la Función Pública DAFP.

 <p>FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA</p> <p>ADMINISTRACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN</p>	<p>SISTEMA INTEGRADO DE GESTIÓN</p> <p>POLÍTICA PARA LA ADMINISTRACIÓN DEL RIESGO DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL</p>		 <p>La salud es de todos</p> <p>Minsalud</p>
<p>VERSIÓN: 1.0</p>	<p>CÓDIGO: ESESDIGPL01</p>	<p>FECHA ACTUALIZACIÓN: 12 DE JULIO 2019</p>	<p>PAGINA 11 DE 20</p>



6.2 NIVELES DE ACEPTACION DEL RIESGO

Los niveles de aceptación del Riesgo pueden ocurrir sin tratamiento, pero los riesgos que sean aceptados en la entidad deberán estar sujetos a monitoreo; los riesgos de corrupción, la tolerancia es inaceptable.

De acuerdo a los criterios manejados por la política de operación del Riesgo del (DAFP.2018) El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia. Establece las bases de los niveles de aceptación de los riesgos con los criterios ERCA - **Evitar, Reducir, Compartir y Asumir**.

- **NIVEL BAJO:** Se **ASUMIRÁ** el Riesgo y administrará por medio de las actividades propias del proceso asociado a su control y registro de avance y se debe presentar en el Informe de Desempeño semestral.
- **NIVEL MODERADO:** Se deberá incluir este riesgo en el Mapa de Riesgos por proceso o gestión, se establecerán acciones de control preventivo que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo, se administrarán mediante seguimiento trimestral y se registrarán sus avances en el formato establecido por parte del ministerio de salud para el monitoreo y seguimiento a los riesgos y se presentara reporte de avance dentro del Informe de Desempeño.
- **NIVEL MAYOR O ALTO:** Se deberá incluir el riesgo en el Mapa de Riesgos Institucional y se establecerán acciones de control preventivo que permitan **EVITAR** la materialización del Riesgo. La administración de estos riesgos tendrá una periodicidad de seguimiento trimestral y su adecuado control se registrará en los Informes de Desempeño.
- **NIVEL EXTREMO:** Se incluirá el riesgo en el Mapa de Riesgos Institucional en el Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia, se establecerán acciones de control preventivo y detectivo que permitan evitar la materialización del riesgo.

Tipo de Riesgo	Zona de Riesgo	Nivel de Aceptación
Riesgos de Gestión	Baja	Se ASUMIRÁ el riesgo y se administra por medio de las actividades propias del proceso se ejecutara con un reporte y seguimiento SEMESTRAL de su desempeño.
	Moderada	Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo, se realizara reporte y seguimiento TRIMESTRAL y se debe registrar sus avances en el mapa de riesgos por proceso.
	Mayor y Extrema	Se debe incluir el riesgo tanto en el mapa de riesgos del proceso o (Gestión) como en el mapa de riesgo institucional y se establecen acciones de control preventivo que permitan MITIGAR la materialización del riesgo y se debe realizar el monitoreo y seguimiento TRIMESTRAL .

<p>Riesgo de Corrupción</p>	<p>Moderada</p>	<p>Se establecen acciones de controles preventivos que permitan REDUCIR la probabilidad de ocurrencia del riesgo. El periodo de seguimiento y monitoreo se realizara TRIMESTRAL para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos y se debe registrar en el Mapa de Riesgos del Proceso o (Gestión) como también en el Mapa de Riesgo Institucional.</p>
	<p>Mayor y Extrema</p>	<p>Se adoptan medidas para: REDUCIR la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. EVITAR Se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo. TRANSFERIR O COMPARTIR una parte del riesgo para reducir la probabilidad o el impacto del mismo. Periodicidad de seguimiento y monitoreo se realizara TRIMESTRAL para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos y se debe registrar en el Mapa de Riesgos del Proceso o (Gestión) como también en el Mapa de Riesgo Institucional.</p>

Cabe aclarar que cada tipo de riesgo (Gestión, Corrupción y Seguridad de la Información) Cuenta con un criterio diferenciador de valoración de impacto y este se encuentra descrito en la **GUÍA POLÍTICA PARA LA ADMINISTRACIÓN DEL RIESGO DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL ESDSDIGGS02**.

6.3 NIVELES PARA CALIFICAR EL IMPACTO DEL RIESGO

La escala establecida en el FPS-FNC para calificar el nivel de impacto frente a la materialización del riesgo se realizara de acuerdo a las respuestas, cuya escala es la siguiente:

Para el caso de los riesgos de gestión:

NIVEL	ESCALA	DESCRIPCIÓN
1	INSIGNIFICANTE	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
2	MENOR	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
3	MODERADO	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
4	MAYOR	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad.
5	CASTASTRÓFICO	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

Para el caso de los riesgos de corrupción.

NIVEL	ESCALA	DESCRIPCIÓN	RESPUESTAS AFIRMATIVAS
1	MODERADO	Genera medianas consecuencias sobre la entidad.	1 a 5

6.4 NIVELES DE AUTORIDAD Y RESPONSABILIDAD

Los niveles de autoridad y responsabilidad para la administración del riesgo en el FPS-FNC, está determinado por las líneas de defensa establecidas mediante el Modelo Integrado de Planeación y Gestión MIPG, de la siguiente manera:

 <p>FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA</p> <p>ADMINISTRACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN</p>	<p>SISTEMA INTEGRADO DE GESTIÓN</p> <p>POLÍTICA PARA LA ADMINISTRACIÓN DEL RIESGO DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL</p>		 <p>La salud es de todos Minsalud</p>
<p>VERSIÓN: 1.0</p>	<p>CÓDIGO: ESDSDIGPL01</p>	<p>FECHA ACTUALIZACIÓN: 12 DE JULIO 2019</p>	<p>PAGINA 16 DE 20</p>

LINEAS DE DEFENSA / RESPONSABLES	RESPONSABILIDAD
<p>LINEA ESTRATEGICA</p> <p>Como lo establece el MIPG los funcionarios que hacen parte de la LÍNEA ESTRATÉGICA de la dimensión 7 Control Interno son:</p> <p>La alta dirección (Director General, secretario General y Subdirectores)</p> <p>Miembros del Comité Institucional de Coordinación de Control Interno, la Resolución No. 0538 de abril/2018:</p> <p>Director General, Secretario General, Subdirector de Prestaciones Sociales, Subdirector Financiero, Jefe de la Oficina Asesora Jurídica, Jefe de la Oficina Asesora de Planeación y Sistemas y Jefe de la Oficina de Control Interno.</p>	<ul style="list-style-type: none"> • Establecer y aprobar la Política de riesgo. • Analizar los cambios en el entorno (Interno y Externo). • Revisar del adecuado desdoblamiento de los objetivos institucionales a los objetivos de procesos, que han servido de base para llevar a cabo la identificación de los riesgos. • Hacer seguimiento en el Comité Institucional y de Control Interno a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna. • Revisar el cumplimiento a los objetivos institucionales y de procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos. • Hacer seguimiento y pronunciarse por lo menos cada trimestre sobre el perfil de riesgo inherente y residual de la entidad, incluyendo los riesgos de corrupción y de acuerdo a las políticas de tolerancia establecidas y aprobadas. • Revisar los informes presentados por lo menos cada trimestre de los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos. • Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento. • Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento.
<p>PRIMERA LÍNEA DE DEFENSA</p> <p>Como lo establece el MIPG los funcionarios que hacen parte de la PRIMERA LÍNEA DE DEFENSA de la dimensión 7 Control Interno son:</p> <p>Gerentes públicos (Secretario General, Subdirectores) Líderes de Procesos Gerentes operativos de Programas y Proyectos.</p>	<ul style="list-style-type: none"> • Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos, para la actualización de la matriz de riesgos de su proceso. • Revisión como parte de sus procedimientos de supervisión, la revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos. • Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos. • Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos. • Revisar y reportar a planeación, los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas a través del análisis de indicadores asociados a dichos objetivos. • Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento a los objetivos. • Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con las líneas estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos.

 <p>FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA</p> <p>ADMINISTRACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN</p>	<p>SISTEMA INTEGRADO DE GESTIÓN</p> <p>POLÍTICA PARA LA ADMINISTRACIÓN DEL RIESGO DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL</p>	 <p>La salud es de todos Minsalud</p>
<p>VERSIÓN: 1.0</p>	<p>CÓDIGO: ESESDIGPL01</p>	<p>FECHA ACTUALIZACIÓN: 12 DE JULIO 2019</p>
<p>PAGINA 17 DE 20</p>		

LINEAS DE DEFENSA / RESPONSABLES	RESPONSABILIDAD
<p>SEGUNDA LÍNEA DE DEFENSA</p> <p>Como lo establece el MIPG los funcionarios que hacen parte de LA SEGUNDA LÍNEA DE DEFENSA de la dimensión 7 Control Interno son:</p> <p>Jefe de la Oficina Asesora de Planeación y Sistemas Coordinadores de Grupos Internos de Trabajo, Supervisores e interventores de contratos</p> <p>Integrantes del Equipo Interdisciplinario de Apoyo a la implementación MIPG y Mejoramiento del Sistema de Control Interno</p>	<ul style="list-style-type: none"> • Revisar los cambios en el direccionamiento estratégico o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar y apoyar en la actualización de las matrices de riesgos. • Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar. • Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y determinar las recomendaciones y seguimiento para el fortalecimiento de los mismos. • Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad. • Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos. • Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos.
<p>TERCERA LINEA DE DEFENSA</p> <p>Oficina de Control Interno o quien haga sus veces.</p>	<ul style="list-style-type: none"> • Revisar los cambios en el “Direccionamiento estratégico” o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables. • Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar. • Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, además de incluir los riesgos de corrupción. • Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos. Revisar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas. • Para mitigar los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos y los planes de mejora como resultado de las auditorías efectuadas, además, que se lleven a cabo de manera oportuna, se establezcan las causas raíz del problema y se evite, en lo posible, la repetición de hallazgos y la materialización de los riesgos.

 <p>FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA</p> <p>ADMINISTRACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN</p>	<p align="center">SISTEMA INTEGRADO DE GESTIÓN</p> <p align="center">POLÍTICA PARA LA ADMINISTRACIÓN DEL RIESGO DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL</p>		 <p>La salud es de todos Minsalud</p>
<p>VERSIÓN: 1.0</p>	<p>CÓDIGO: ESDSDIGPL01</p>	<p>FECHA ACTUALIZACIÓN: 12 DE JULIO 2019</p>	<p>PAGINA 18 DE 20</p>

6.5 TRATAMIENTO DEL RIESGO:

Para la definición e implementación de las acciones establecidas a orientar a la entidad en cuanto a aceptar, evitar, reducir o compartir el riesgo identificado en el FPS-FNC se deberán analizar y evaluar la viabilidad técnica, jurídica y financiera para su implementación. Las alternativas que tendrá el FPS-FNC para el tratamiento de los riesgos serán:

ACEPTAR EL RIESGO:

Si el nivel de riesgo cumple con los criterios de aceptación de riesgo, no es necesario poner controles y el riesgo puede ser aceptado. Esto debería aplicar para riesgos inherentes en la zona de calificación de riesgo bajo.

La aceptación del riesgo puede ser una opción viable según las políticas de administración de los riesgos en el **Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia**, con respecto a los riesgos bajos, como también pueden existir escenarios de riesgos a los que no se le puedan aplicar controles y por ende, se acepta el Riesgo. En ambos escenarios debe existir un seguimiento continuo de los Riesgos. Los riesgos de corrupción en la entidad no son aceptados siguiendo los lineamientos establecidos por la Secretaría de Transparencia de la Presidencia de la República

EVITAR EL RIESGO:

Cuando los escenarios de riesgo identificado se consideran extremos, se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o conjunto de actividades.

Desde el punto de vista de los responsables de la toma de decisiones, este tratamiento de evitar el riesgo es simple, la menos arriesgada y menos costosa, pero es un obstáculo para el desarrollo de las actividades de la entidad y por lo tanto hay situaciones donde no es una opción.

COMPARTIR EL RIESGO:

Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable, o se carece de conocimientos necesarios para gestionarlo, el riesgo puede ser compartido con otra parte interesada (Ministerio de Salud y Protección Social, Ministerio de Hacienda y Crédito Público, IPS de la Red prestadora, Contratistas, Agencias de Seguros) que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.

Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización. Estos mecanismos de transferencia de riesgos deben estar formalizados a través de un acuerdo contractual.

 <p>FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA</p> <p>ADMINISTRACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN</p>	<p align="center">SISTEMA INTEGRADO DE GESTIÓN</p> <p align="center">POLÍTICA PARA LA ADMINISTRACIÓN DEL RIESGO DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL</p>		 <p>La salud es de todos Minsalud</p>
<p>VERSIÓN: 1.0</p>	<p>CÓDIGO: ESESDIGPL01</p>	<p>FECHA ACTUALIZACIÓN: 12 DE JULIO 2019</p>	<p>PAGINA 19 DE 20</p>

REDUCIR EL RIESGO:

El nivel de riesgo debe ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.

Deben seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado, logre la reducción prevista sobre el riesgo.

Para mitigar/tratar los riesgos de seguridad digital, se deben emplear como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, los cuales igualmente se encuentran en el Anexo 4. “Lineamientos para la gestión del riesgo de seguridad digital de la presente guía”.

Tratamiento del Riesgo – Rol de la Primera Línea de Defensa o (Líderes de los procesos):

Como medio para propiciar el logro de los objetivos en los procesos del Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia, se deben realizar las actividades de controles orientadas a prevenir y detectar la materialización de los riesgos. Se considera que la efectividad de los controles depende del grado de cumplimiento de los objetivos estratégicos y de proceso de la entidad. Por lo tanto se considera como responsabilidad según el D.A.F.P 2018 a la primera línea de defensa o (líderes de los proceso) el establecimiento de actividades de control.

6.6 GESTION DE ACCIONES CORRECTIVAS Y PLANES DE TRATAMIENTO DEL RIESGO

Las acciones establecidas para la administración y tratamiento del riesgo se deben cumplir conforme a los lineamiento establecidos en la GUÍA POLÍTICA PARA LA ADMINISTRACIÓN DEL RIESGO DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL ESESDIGGS02 y en el procedimiento ADMINISTRACIÓN DEL RIESGO PEMYMOPSP06, con un enfoque por procesos basados en la eliminación de las causas y en el fortalecimiento de los controles.

Para el caso de los riesgos de corrupción se cumplirá según lo establecido en la metodología para la administración de los riesgos de corrupción y atención al ciudadano PAAC.

 <p>FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA</p> <p>ADMINISTRACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN</p>	<p>SISTEMA INTEGRADO DE GESTIÓN</p> <p>POLÍTICA PARA LA ADMINISTRACIÓN DEL RIESGO DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL</p>		 <p>La salud es de todos</p> <p>Minsalud</p>
<p>VERSIÓN: 1.0</p>	<p>CÓDIGO: ESESDIGPL01</p>	<p>FECHA ACTUALIZACIÓN: 12 DE JULIO 2019</p>	<p>PAGINA 20 DE 20</p>