FONDO DE PASIVO SOCIAL
FERROCARRILES NACIONALES DE COLOMBIA

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CONTROL DE DOCUMENTOS			
Elaboró: SOL MARINA CURE FLOREZ	**Cargo:** Profesional encargado	**Fecha:** 19/02/2025	**Firma:**
Revisado técnicamente en O.P.S: Sebastián Andrés Marimón Padilla	**Cargo:** Contratista – Profesional de Apoyo OPS	**Fecha:** 24/02/2025	**Firma:**
Aprobado mediante: **Acta:** **Acto Administrativo:** **Fecha**	**05/2025** **RESOLUCIÓN 496 /2025** **20/3/2025**		

CONTROL DE CAMBIOS			
Versión	**Fecha y acto administrativo de aprobación**	**Cambio**	**Solicitante**
1.0	Resolución 0846 de 2017	Documento nuevo	
2.0	Resolución1680 2/8/2023	Actualización de política de acuerdo a nuevos requerimientos legales para la implementación de un SGSI alineado con el MPSI de MINTIC	María Yaneth Farfán
3.0	Resolución 496 20/3/2025	Actualización de política en alineación con el MSPI de MINTIC	

CONTENIDO

INTRODUCCIÓN

El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia considera que la información es uno de sus principales activos intangibles indispensable en el cumplimiento de su misión y en la dirección y consecución de sus objetivos, programas, planes, proyectos y metas, por lo que se hace necesario establecer estrategias y mecanismos que nos permita protegerla independientemente del medio en que se encuentre o la forma en que se maneje, transporte o almacene.

Esta política está alineada con el Modelo de Seguridad y Privacidad de la Información (MSPI) establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones, asegurando la confidencialidad, integridad y disponibilidad de la información, esenciales para la misión de la organización.

La seguridad de la información es una prioridad para el Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia (FPS-FNC), por tanto, es responsabilidad de todos los empleados, contratistas y terceros el cumplimiento de cada una de estas políticas y lineamientos, acorde con la normatividad vigente.
Las políticas del sistema de gestión de seguridad de la información (SGSI) se definen según su orden de importancia en:
Primer Nivel: Corresponde a la Política General del Sistema de Gestión de Seguridad de la Información (SGSI), la cual es una directriz global que establece qué y por qué se quiere proteger. Su definición y actualización está alineada con la planeación estratégica del FPS-FNC. Establece las responsabilidades generales aplicables a toda la entidad en lo que respecta a la temática de Seguridad de la Información.
Segundo Nivel: Corresponde al Manual de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo.
Tercer Nivel: Corresponde a políticas específicas enfocadas a grupos, servicios o actividades particulares. Su definición y actualización debe reflejar cambios de índole organizacional y tecnológica.

1. OBJETIVO

El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia (FPS-FNC) establece la presente política con el objetivo de proteger la confidencialidad, integridad, disponibilidad y privacidad de sus activos de información. A través de controles administrativos y operativos, se busca garantizar un entorno seguro y

confiable para el tratamiento de la información, asegurando el cumplimiento de las normativas y regulaciones aplicables.

1.1 OBJETIVOS ESPECÍFICOS

- ✔ Gestionar los activos de información del FPS-FNC, mediante su identificación, clasificación y protección, garantizando la confidencialidad, integridad y disponibilidad a través de controles diseñados para mitigar riesgos y responder a las necesidades de seguridad de la entidad.
- ✔ Promover una cultura organizacional de seguridad de la información, asegurando que cada miembro del equipo esté consciente y comprometido con las mejores prácticas y lineamientos de seguridad, reflejando un entorno de trabajo seguro y responsable.
- ✔ Afrontar las amenazas y ataques cibernéticos de los que es objeto la infraestructura del Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia (FPS-FNC), mediante la correcta gestión de eventos e incidentes de seguridad de la información.

2. ALCANCE

Esta política aplica a toda la entidad, sus servidores públicos, contratistas, terceros, proveedores del Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia (FPS-FNC) y la ciudadanía en general, asegurando la protección y manejo adecuado de la información.

3. BASES LEGALES

El marco legislativo y regulatorio en el cual se delimita el Sistema de Gestión de Seguridad de la Información del Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia (FPS-FNC) incluye:

- Ley 1581 DE 2012. Por la cual se dictan disposiciones generales para la protección de datos personales
- 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.
- Resolución 500 DE MARZO 10 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”
- Decreto 767 de 2022, Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital.

- 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

4. DEFINICIONES

Activo

En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Amenazas

Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría

Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

Ciberseguridad

Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio

Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de la Academia de la lengua española).

Confidencialidad

Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. (ISO/IEC 27000).

Control

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Declaración de aplicabilidad
Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Disponibilidad
Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. (ISO/IEC 27000).

Gestión de incidentes de seguridad de la información
Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Integridad es la propiedad que garantiza la exactitud y completitud de los activos de información y su protección contra modificaciones no autorizadas. (ISO/IEC 27000).

Parte interesada (Stakeholder)
Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

Plan de continuidad del negocio
Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos
Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Privacidad

Se define como el derecho de los individuos a controlar o influir sobre la forma en que se recopila, procesa, almacena y comunica su información personal. Esto incluye la protección de los datos personales contra el acceso, uso y divulgación no autorizados, así como el cumplimiento de las normas y regulaciones que salvaguardan los derechos de los individuos en relación con sus datos personales.

Riesgo
Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información
Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI
Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Trazabilidad
Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Vulnerabilidad
Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

5. POLÍTICA GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

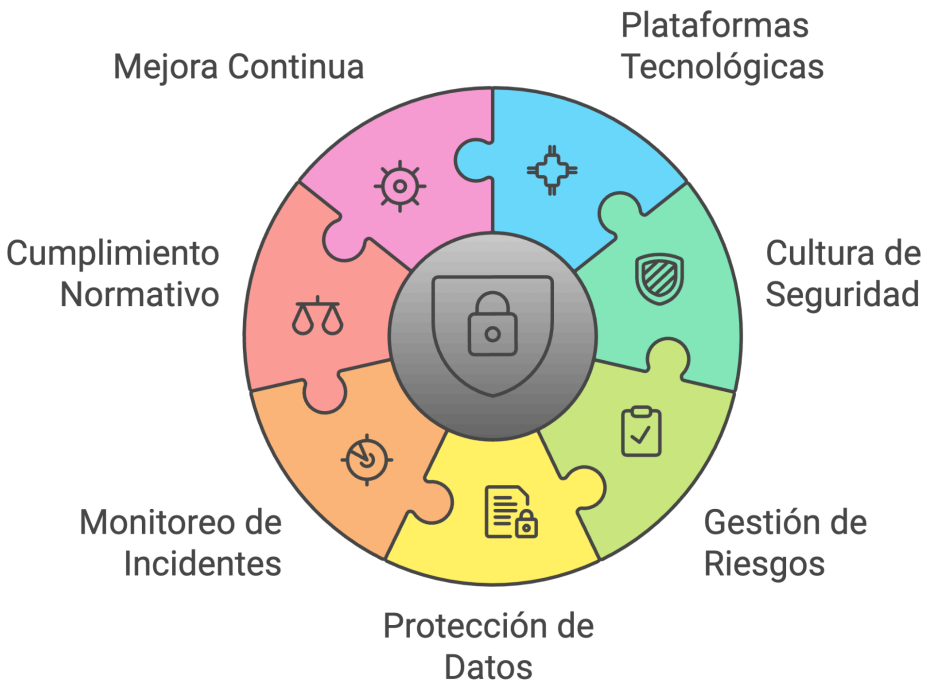
El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia (FPS-FNC) asume el compromiso de implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI), fundamentado en la protección integral de sus activos de información y en el cumplimiento de sus deberes institucionales. Este sistema es un pilar esencial para garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información, fortaleciendo la confianza de todos los actores involucrados.

El SGSI tiene como objetivo la formulación, adopción, implementación y monitoreo de políticas, normativas, planes y proyectos dirigidos a proteger la información del FPS-FNC en el contexto del Sector Salud y Protección Social. Esta política se extiende a todos los niveles de la entidad, incluyendo a sus servidores públicos, contratistas, terceros y la ciudadanía en general, asegurando el cumplimiento de los requisitos legales e institucionales aplicables y promoviendo una cultura de seguridad de la información.

A través del diseño y ejecución de controles, la identificación de amenazas y la gestión proactiva de riesgos, el FPS-FNC se compromete a establecer lineamientos claros para el tratamiento seguro de la información, que permitan su continua mejora y adaptación a las nuevas exigencias tecnológicas y regulatorias.

La Política General de Seguridad del sistema de gestión de la Información estará determinada por las siguientes premisas:

Estrategia Integral de Seguridad de la Información



1. Disponer de plataformas tecnológicas apropiadas que respalden el procesamiento, almacenamiento y comunicación de la información, facilitando la protección de servicios críticos como el registro, validación y gestión de trámites del Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia (FPS-FNC).

2. Fortalecer la cultura y competencias en Seguridad de la Información de servidores públicos, contratistas, terceros y proveedores de la entidad; promoviendo que cada actor comprenda y aplique los principios de protección de la información en sus actividades diarias.

3. Implementar y mantener una metodología actualizada de gestión de riesgos de seguridad de la información que permita anticiparse a situaciones que puedan afectar la disponibilidad, confidencialidad e integridad de la información del Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia (FPS-FNC), de acuerdo con los lineamientos establecidos en la regulación legal vigente, normas y buenas prácticas nacionales e internacionales para la gestión adecuada de riesgos.

4. Implementar lineamientos específicos para la protección de datos personales, en cumplimiento con la legislación de privacidad, promoviendo prácticas responsables en el manejo y tratamiento de datos personales sensibles y no sensibles.

5. Diseñar un proceso de monitoreo constante y gestión de incidentes de seguridad que permita detectar y responder a amenazas de manera oportuna, minimizando el impacto en la operación y en los activos de información del FPS-FNC.

6. Cumplir con la normatividad vigente, manteniendo el SGSI en conformidad con las regulaciones y adaptando sus controles y prácticas de acuerdo con las exigencias legales.

7. Fomentar la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), optimizando los procesos y controles en función de los cambios tecnológicos y regulatorios.

6. POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia (FPS-FNC) considera la información un activo de alta importancia para la Entidad, esencial para el desarrollo continuo de su misión y el cumplimiento de sus objetivos. En consecuencia, es necesario definir e implementar lineamientos que permitan proteger la confidencialidad, integridad y disponibilidad de la información en todo el ciclo de vida.

Para este propósito, el FPS-FNC establece el documento *APGTS-OPS-MS-01 Manual del sistema de gestión de la seguridad y privacidad de la información*, el cual contiene las políticas específicas de seguridad de la información. Estas políticas deben ser adoptadas por los servidores públicos, contratistas, terceros y proveedores que presten sus servicios o tengan algún tipo de relación con la entidad.

7. CUMPLIMIENTO

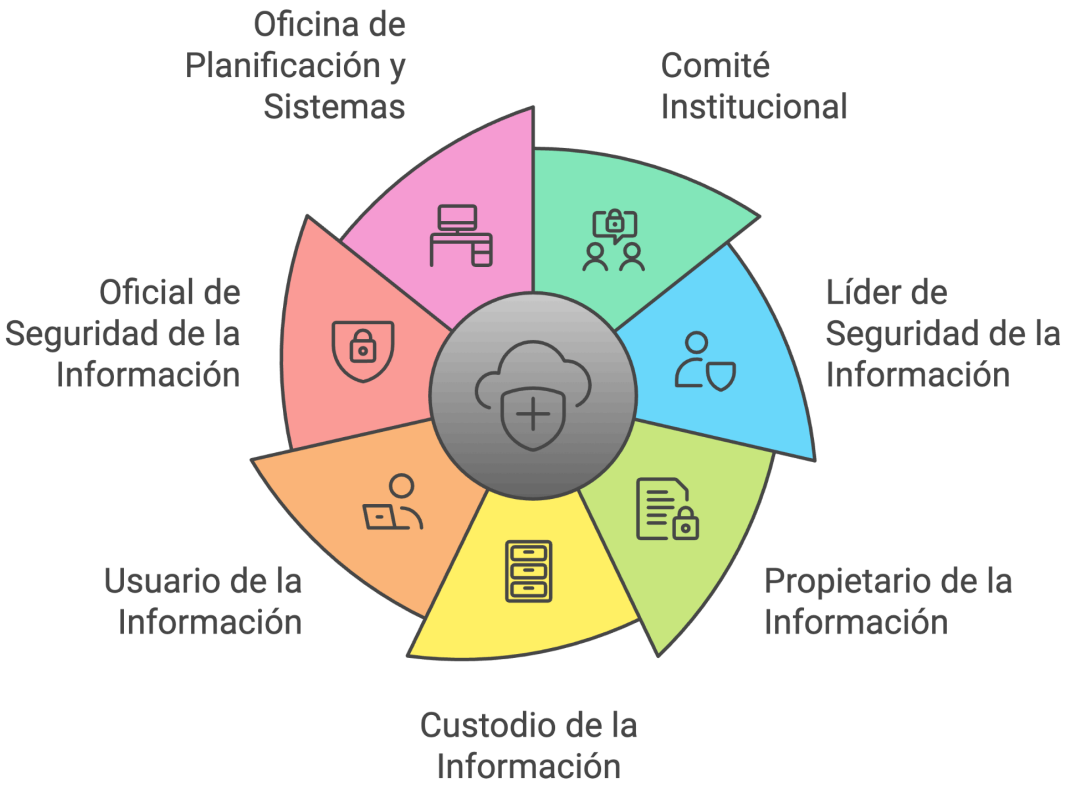
La Política General del Sistema de Seguridad y Privacidad de la Información es mandataria a todo nivel, por lo tanto, debe ser cumplida por los servidores públicos, contratistas, terceros, proveedores que interactúen con los activos de información para el desempeño de sus funciones y contratos.

El Líder del Sistema de Gestión de Seguridad de la Información es responsable de supervisar la implementación y el cumplimiento de esta política, incluyendo el establecimiento de procesos para manejar

desviaciones y excepciones. Este rol implica evaluar el impacto de dichas desviaciones, gestionar los riesgos asociados y garantizar que todas las excepciones estén debidamente autorizadas y documentadas para mantener la integridad del sistema de seguridad de la información.

8. ROLES Y RESPONSABILIDADES

Descripción de los Roles de Seguridad de la Información



- **Comité Institucional de Gestión y Desempeño:** De acuerdo a la resolución 3021 de 2019, es responsable de: Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.

- **Líder del Sistema de Gestión de Seguridad de la Información:** Encargado de integrar los aspectos estratégicos y tácticos del SGSI, y es el representante del SGSI ante el Comité de Institucional de Gestión y Desempeño.

- **Propietario o dueño de la Información:** Responsable de los procesos internos de la entidad, asegurando la protección de la información generada y utilizada en sus operaciones.

- **Custodio de la Información:** En el FPS-FNC los encargados de la custodia de la información son los procesos de Gestión Documental y Gestión de TIC 'S quienes tienen la responsabilidad de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido.

- **Usuario de la Información:** Son todos los funcionarios, proveedores, contratistas y terceros, que, con la debida autorización del propietario de la información, pueden consultar, ingresar, modificar o eliminar información en medios físicos o digitales, a través de las redes y sistemas de información de la entidad.

- **Oficial de Seguridad de la Información:** Responsable de coordinar las actividades de planeación, implementación, revisión y mantenimiento del SGSI, ejecutando las directrices del Comité de Gestión y del Líder del SGSI en los aspectos tácticos y operativos.

- **Oficina Asesora de Planeación y Sistemas:** La Oficina Asesora de planeación y sistemas, en coordinación con el Líder del Sistema de Gestión de Seguridad de la Información, estará encargada de la gestión documental del SGSI perteneciente al sistema integrado de Gestión del FPS FNC.

La descripción específica de estos roles y responsabilidades se encuentran documentadas en el documento APGTSOPSGSO3 Guía roles y responsabilidades del SGSI.

9. DIFUSIÓN, REVISIÓN, CUMPLIENTO, VIGENCIA

9.1 DIFUSIÓN

El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia (FPS - FNC) comunicará todas las políticas, procedimientos u otros documentos generados en el marco del Sistema de Gestión de Seguridad de la Información a través de los siguientes canales de comunicación: correo electrónico, intranet, comunicaciones impresas, charlas y/o capacitaciones y aplicativo del SIG FPS. Serán publicados en la intranet y página web del FPS - FNC a través del link respectivamente y se le informará a cada funcionario a través de correo masivo u otras actividades de difusión que se definan para tal efecto.

Será responsabilidad del proceso de Gestión de Talento Humano incorporar la aplicación y observancia de las Políticas de Seguridad y Privacidad de la información, en el plan de capacitación institucional, y velar por la correcta inducción y reinducción de los funcionarios en materia de seguridad y privacidad de la información.

Será responsabilidad de la oficina asesora jurídica incorporar dentro de los contratos, la cláusula de cumplimiento de las Políticas de Seguridad y Privacidad de la Información, la cual debe ser entregada para su consentimiento y firma de esta.

El jefe de la oficina asesora de planeación y sistemas será el responsable de la existencia permanente y el cumplimiento de un plan formal de difusión, capacitación y sensibilización de la seguridad de la información.
El oficial de Seguridad de la información es el responsable de la ejecución del plan y el cumplimiento de sus objetivos, así como la existencia de un plan de comunicación que lo complemente.

9.2 REVISIÓN

La Política General de Seguridad y Privacidad de la información será revisada y evaluada en su cumplimiento de manera anual o cuando requiera modificaciones con el objetivo de mantenerla actualizada.

Esta revisión y evaluación será liderada por gestión TIC'S, revisado por la oficina de planeación y sistemas, y aprobado por el comité de desarrollo administrativo, considerando los siguientes aspectos:

- Condiciones contractuales, regulatorias y legales.
- Cambios en ámbito organizacional o técnico.
- Disponibilidad de recursos.
- Retroalimentación de las partes interesadas.
- Resultados de las revisiones efectuadas por terceras partes.
- Estados de acciones preventivas y correctivas.
- Alertas ante amenazas y vulnerabilidades.
- Información relacionada a incidentes de seguridad.
- Medición de los indicadores del Sistema de Gestión de Seguridad de la Información.

9.3 CUMPLIMIENTO

Todas las personas cubiertas por el alcance y aplicabilidad se deberán adherir en un 100% a la política de seguridad de la información, establecida por el FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA.

Los funcionarios que infrinjan esta política; serán sujetos a la aplicación de la normatividad de tipo disciplinario y penal vigente.

9.4 VIGENCIA

La presente política rige a partir de la fecha de su resolución de adopción en el Sistema Integrado de Gestión.