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:** **02-05-2023**	**Firma:** *Sol Cure*
Revisado técnicamente en O.P.S CAMILO RODRIGUEZ	**Cargo:** CONTRATISTA	**Fecha:** **22-06-2023**	**Firma:** *Camilo Rodríguez*
Aprobado mediante: **Acta:** **Acto Administrativo:** **Fecha**	 **07/2023** **Resolución 1680** **2/8/2023**		

CONTROL DE CAMBIOS			
Versión	**Fecha y acto administrativo de aprobación**	**Cambio**	**Solicitante**
1.0	Resolución 0846 de 2017	Documento nuevo	
2.0	Resolución 1680 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

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 permitan protegerla independientemente del medio en que se encuentre o la forma en que se maneje, transporte o almacene.

Para el Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia (FPS-FNC), la seguridad y privacidad de la información busca la disminución en el impacto generado sobre sus activos de información, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

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

Determinar los lineamientos a través del establecimiento de políticas reglamentarias, controles administrativos y operativos sobre el buen uso de la información que permitan proteger los activos de información del Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia (FPS-FNC) apoyado en mecanismos de aseguramiento que permitan el cumplimiento de la confidencialidad, privacidad, integridad y disponibilidad de la información del (FPS-FNC).

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.

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:

- Norma Técnica Colombiana NTC-ISO-IEC-27001 Sistemas de Gestión de la Seguridad de la Información (SGSI).
- 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 auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (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.

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.

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).

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).

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).

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.

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 el Sistema de Gestión de Seguridad de la Información, destacando la importancia de una gestión adecuada de la información y el fortalecimiento de la confianza en el cumplimiento del deber institucional, cuyo objetivo es la formulación, adopción, implementación, y seguimiento de las políticas, regulaciones, reglamentaciones, planes, programas y proyectos del Sector Salud y Protección Social. Esta política aplica a toda la entidad, sus servidores públicos, contratistas y terceros del FPS-FNC y la ciudadanía

en general, buscando la protección de los activos de seguridad de la información, a través del cumplimiento de los requisitos legales e institucionales, así como la generación e implementación de lineamientos para el óptimo tratamiento de la información y complementado con el diseño de controles, identificación y gestión de riesgos.

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

1. Contar con plataformas apropiadas que protejan los mecanismos de procesamiento, almacenamiento y comunicación donde están contenidos y soportados todos los servicios, registro, validación y realización de trámites del Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia (FPS-FNC).
2. Fortalecer la cultura y competencias de los servidores públicos, contratistas, terceros, proveedores de la entidad respecto a la gestión de Seguridad de la Información.
3. Implementar y mantener actualizada una metodología de gestión de riesgos de seguridad de la información como herramienta para actuar proactivamente ante la presencia de 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 correcta gestión de riesgos.
4. Implementar y mantener la mejora continua del sistema de gestión de la seguridad de la seguridad de la información

Objetivos específicos

I. Gestionar los activos de seguridad de la información del FPS-FNC en cuanto a su identificación, clasificación y protección para preservar su confidencialidad, integridad y disponibilidad.
II. Sensibilizar al personal para lograr servidores públicos competentes y comprometidos con una cultura de seguridad de la información reflejada en la aceptación y aplicación de las directrices de seguridad establecidas por la entidad.
III. Mantener en constante mejora y evaluación el Sistema de Seguridad de la Información, aplicando las acciones consideradas para el sostenimiento del mismo.
IV. Afrontar las amenazas y ataques digitales (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.

6. POLÍTICAS ESPECIFICAS DE SEGURIDAD DE LA INFORMACIÓN

El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia (FPS-FNC) determina la información como un activo de alta importancia para la Entidad, el cual permite el desarrollo continuo de la misión y el cumplimiento del objetivo de la misma, generando la necesidad de implementar reglas y medidas que permitan identificar los riesgos y proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información, razón por la cual el FPS-FNC establece el documento (APGTSOPSPTMS01) Manual del sistema de gestión de la seguridad y privacidad de la información, el cual contiene las políticas específicas de seguridad de la información las cuales deben ser adoptadas por los servidores públicos, contratistas,

terceros, proveedores que presten sus servicios o tengan algún tipo de relación con la entidad; estas políticas se encuentran enfocadas al cumplimiento de la normatividad legal Colombiana relacionadas con la seguridad de la información y a las buenas prácticas de seguridad de la información.

7. CUMPLIMIENTO

La Política General del Sistema de Gestión de Seguridad 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.

8. ROLES Y RESPONSABILIDADES

- **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:** esta a cargo de la integración entre los aspectos estratégicos y tácticos que se presenten en el SGSI. Es el representante del SGSI ante el Comité de Institucional de Gestión y Desempeño.

- **Propietario o dueño de la Información:** Es el encargado de los procesos dentro de la entidad, los cuales, son responsables de la información que se genera y se utiliza en las operaciones de sus procesos.

- **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 borrar en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la entidad.

- **Oficial de Seguridad de la Información:** Se encarga de coordinar la ejecución de las actividades derivadas de la planeación, implementación, revisión y mantenimiento del SGSI. Coordina el aspecto táctico y operativo ejecutando las directrices del comité de gestión y desempeño y del líder del Sistema de Gestión.

- **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.

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 materias 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 In 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, este proceso será liderado 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 antes 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.