PLAN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Fecha de Vigencia: 26/12/2019

CONTROL DE DOCUMENTOS			
Elaboró: SOL MARINA CURE FLOREZ	**Cargo:** Profesional de apoyo a la gestión de la Oficina Asesora de Planeación y Sistemas	**Fecha:**	**Firma:**
Revisado técnicamente en O.P.S **CAMILO JOSÉ RODRIGUEZ C**	**Cargo:** Profesional encargado	**Fecha:**	**Firma:**
Aprobado mediante: **Acta:** **Acto Administrativo:** **Fecha**			

CONTROL DE CAMBIOS			
Versión	**Fecha y acto administrativo de aprobación**	**Cambio**	**Solicitante**
1.0		Documento nuevo	So Marina Cure / María Yaneth Farfán Casallas

Contenido

1. INTRODUCCIÓN

De acuerdo al decreto 612 de 2018 donde se determinan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado, y donde se exige la elaboración del Plan de Seguridad y Privacidad de la Información mediante Decreto 1078 de 2015 en el artículo 2.2.9.1.2.2, como instrumentos para la implementación de estrategia de gobierno en línea, por ello el Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia en cumplimiento a las anteriores directrices y en contribuir en la implementación de la política digital que permite tener un estado más eficiente y transparente propone el siguiente plan de seguridad y privacidad de la información, donde le permita a la entidad priorizar y enfocar estratégicas en aseguramiento de la información de nuestros pensionados y beneficiarios de la empresa liquidada Ferrocarriles Nacionales.

2. OBJETIVO GENERAL

Establecer el plan de seguridad y privacidad de la información para la construcción del sistema de gestión de seguridad y privacidad del la información del Fondo de Pasivo Social de Ferrocarriles Nacionales de acuerdo a los lineamientos de la política de gobierno digital y el modelo integrado de gestión para preservar la confidencialidad, integridad y disponibilidad de la información relacionada con pensionados y beneficiarios de la empresa liquidada Ferrocarriles Nacionales.

3. OBJETIVOS ESPECÍFICOS

- Definir las actividades para establecer la estrategia de seguridad de la información de la entidad.
- Apalancar la implementación del Sistema de Gestión de Seguridad de la Información de la entidad de acuerdo con los requerimientos establecidos en el modelo de seguridad de la estrategia de Gobierno Digital.
- Establecer lineamientos para la implementación y adopción de mejores prácticas de seguridad en la entidad.

4. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Este documento aplica para la formulación y seguimiento de actividades como apoyo al Sistema de Gestión de Seguridad de la Información del Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia, abarca a todos los procesos que conforman la entidad, involucrando los misionales (Gestión de Servicio Salud, Gestión de Prestaciones Económicas y Atención al Ciudadano), estratégicos (Direccionamiento Estratégico), de apoyo (Gestión de Recursos Financieros , Gestión de Servicios Administrativos, Gestión de Talento Humano, Gestión de TIC, Gestión de Cobro , Asistencia Jurídica, Gestión de Bienes Transferidos y Gestión

Documental) y los de evaluación (Seguimiento y Evaluación Independiente y Medición y Mejora) y así como aquellos procesos externos que estén vinculados por contratos o acuerdos con terceros los cuales son relevantes en la prestación del servicio.

El Sistema de gestión de seguridad y privacidad de la información aplica para la sede principal de la entidad, ubicada en la ciudad de Bogotá y puntos administrativos fuera de ella, limitando las actividades que se desarrollan en estos puntos.

5. BASES LEGALES

- **Conpes 3854 de 2016**, objetivo general "Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país".

- **Ley 1581 de 2012, Articulo 17 _Item d** "Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento"

- **Ley 1712 de 2014,** Principio de transparencia: Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta ley se presume pública, en consecuencia de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta ley.

- **Ley 1712 de 2014, artículo 7:** Disponibilidad de la información: En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la Web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten.

- **Decreto 2573 de 2014**: "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea…" donde se encuentra como componente el modelo de Seguridad y Privacidad de la Información.

- **Decreto 1413 de 2007, Seguridad de la información.** Los actores que traten información, en el marco del presente título, deberán adoptar medidas apropiadas, efectivas y verificables de seguridad que le permitan demostrar el correcto cumplimiento de las buenas prácticas consignadas en el modelo de seguridad y privacidad de la información emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones, o un sistema de gestión de seguridad de la información certificable. Esto con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información.

- **Decreto 1499 de 2017, Titulo 22, Capitulo 1, artículo 2.2.22.1.5.** ***Articulación y complementariedad con otros sistemas de gestión.*** El Sistema de Gestión se complementa y articula, entre otros, con los Sistemas Nacional de Servicio al Ciudadano, de Gestión de la Seguridad y Salud en el Trabajo, de Gestión Ambiental y de Seguridad de la Información.

- **Decreto 612 de 2018**, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

- **Decreto1008 de 2018 ,**Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

6. 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

Principio de seguridad de la información, el cual asegura que el acceso a la información está adecuadamente autorizado.

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

Principio de seguridad de la información, que tiene por objetivo asegurar que los usuarios autorizados pueden acceder a la información cuando la necesitan".

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

Principio de seguridad de la información, que garantiza que los datos no han sido modificados desde su creación sin autorización.

No repudio

En seguridad de la información, el no repudio garantiza la participación de las partes en una comunicación (emisor y receptor), garantiza que la persona que envía el mensaje no puede negar que es el emisor del mismo y que el receptor no puede negar que recibió el mensaje.

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).

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.

7. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.
Para el Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia (FPS- FNC), la seguridad y privacidad de la información busca proteger, preservar y administrar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información mediante una gestión integral de riesgos y la implementación de controles físicos y digitales previniendo así incidentes de seguridad.

8. OBJETIVOS ESPECIFICOS DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

- Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad, continuidad y no repudio de la información de la entidad
- Definir los lineamientos necesarios para el manejo de la información tanto física como digital en el marco de una gestión documental basada en Seguridad y Privacidad de la Información
- Identificar, gestionar y controlar los riesgos en la seguridad de la información con el fin de determinar controles efectivos.
- Minimizar los incidentes de seguridad de la información.

- Revisar periódicamente el cumplimiento de los requisitos legales que en materia de seguridad y privacidad de la información apliquen a la entidad.
- Generar conciencia de la seguridad y privacidad de la información.
- Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información, seguridad digital y protección de la información personal.
-

9. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

Figura 1 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

9.1. FASE DE DIAGNOSTICO:

Metas	Actividades \ Instrumentos \ Resultados
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad	**Diagnóstico** de la **situación actual** de la entidad con relación a la Gestión de seguridad de la información. **Diagnostico nivel de cumplimiento** de la entidad frente a los objetivos de control y controles establecidos en el Anexo A de la **norma ISO 27001:2013**. **Valoración estado actual** de la gestión de seguridad de la entidad con base en el Instrumento de Evaluación MSPI de MINTIC.
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad.	**Valoración** del **nivel de estratificación** de la entidad frente a la seguridad de la información **con base en** el método planteado en el documento '*ANEXO 3: ESTRATIFICACIÓN DE ENTIDADES*' del modelo seguridad de la información para la estrategia de Gobierno en Línea 2.0.

	Valoración del **nivel de madurez** de seguridad y privacidad de la información en la entidad de acuerdo con los lineamientos establecidos en el capítulo '*MODELO DE MADUREZ*' del documento Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea.
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	**Ejecución prueba de vulnerabilidades** con el fin de identificar el nivel de seguridad y protección de los activos de información de la Entidad y definición de planes de mitigación.

Para la recolección de la información, en esta fase se utilizarán mecanismo como: • Diligenciamiento de cuestionarios con el objetivo de determinar el nivel de cumplimiento de le entidad con relación a los dominios de la norma ISO/IEC 27001:2013. • Documentación existente en el sistema de calidad de la entidad relacionada con la información de las partes interesadas de la entidad y los roles y funciones asociados a la seguridad de la información. • Fuentes externas, como las guías de autoevaluación, encuesta y estratificación dispuestas por la estrategia de gobierno en línea Ministerio de Tecnologías de la Información y las Comunicaciones.

9.2. FASE DE PLANIFICACIÓN:

Metas	Actividades \ Instrumentos \ Resultados
Realizar un análisis de Contexto y factores externos e internos de la Entidad en torno a la seguridad de la información.	**Realizar** un **Análisis de Contexto** de la entidad entorno a la seguridad de la información teniendo en cuenta el capítulo 4. CONEXTO DE LA ORGANIZACIÓN de la norma ISO 27001:2013, con el fin de poder determinar las cuestiones externas e internas de la organización que son pertinentes para la implementación del Sistema de Gestión de Seguridad de la Información.
Definir el alcance del SGSI de la entidad	**Definir** el **alcance** del **Sistema de Gestión de Seguridad de la Información** 'SGSI' de la entidad aprobado por la Alta Dirección y socializado al interior de la Entidad. Definir el alcance del SGSI, en el cual se establece los límites y la aplicabilidad del Sistema de Gestión de Seguridad de la Información.
Definir Roles, Responsables y Funciones de seguridad y privacidad de la información	**Adicionar** las **funciones de seguridad** de la información al **Comité de Riesgos** de la entidad y formalizarlas mediante acto administrativo. **Establecer** el **Rol** de **Oficial de Seguridad** de la información. **Definir** un **marco de gestión que contemple roles y**

	responsabilidades para la implementación, administración, operación y gestión de la seguridad de la información en la entidad. **Definir la estructura organizacional** de la Entidad que contendrá los roles y responsabilidad **pertinentes a la seguridad** de la información.
Definir la metodología de riesgos de seguridad de la información	**Definir Metodología** de Valoración de **Riesgos de Seguridad**. **Integrar** la **metodología** definida con la metodología de riegos operativos de la entidad. **Implementar** un **sistema de información** para la administración y gestión de los riesgos de seguridad de la entidad.
Elaborar las Políticas de seguridad y privacidad de la información de la entidad	**Elaborar Política General de Seguridad y Privacidad** la cual debe ser aprobada por la Alta Dirección y socializada al interior de la Entidad. **Elaborar** el **manual de Políticas de Seguridad y Privacidad de la Información**, que correspo nde a un documento que contiene las políticas y los lineamientos que se implementaran en la Entidad con el objetivo de proteger la disponibilidad, integridad y Confidencialidad de la información. Estas políticas deben ser aprobadas por la Alta Dirección y socializadas al interior de la Entidad.
Elaborar documentación de Operación (formatos de procesos, procedimientos y documentos debidamente definidos y establecidos) del sistema de seguridad de la información	**Elaborar** los **documentos de operación del sistema de seguridad** de la información, tales como: • Declaración de aplicabilidad • Procedimiento y/o guía de identificación y clasificación de activos de información. • Procedimiento Continuidad del Negocio, Procedimientos operativos para gestión de TI • Procedimiento para control de documentos (SGI) • Procedimiento para auditoría interna (SGI) • Procedimiento para medidas correctivas (SGI) • Procedimiento para la gestión de eventos e incidentes de seguridad de la información • Procedimiento para la gestión de vulnerabilidades de seguridad de la información. • Entre otros.

Identificar y valorar activos de información	**Realizar** la **identificación** y **valoración** de los **activos de información** de la entidad de acuerdo con su nivel de criticidad de acuerdo con el alcance del SGSI. Documentar el inventario de activos de información de la entidad.
Identificar, valorar y tratar los riesgos de seguridad de la información de la entidad	**Realizar** la **identificación** y **valoración** de los **riesgos** transversales de **seguridad** de la información y definir los respectivos planes de tratamiento. Realizar la valoración de riesgos de seguridad de la información de acuerdo con el alcance del SGSI. Definir los planes de acción que incluya los controles a implementar con el objetivo de mitigar los riesgos identificados en el proceso de valoración de riesgos. Para la seleccionar de los controles, se tomará como base los objetivos de control y los controles establecidos en el Anexo A de la norma ISO/IEC 27001:2013.
Establecer Plan de capacitación, comunicación y sensibilización de seguridad de la información.	**Elaborar plan** anual de **capacitación** y sensibilización anual de seguridad de la información
Establecer Plan de diagnóstico de IPv4 a IPv6	**Realizar** el **diagnóstico** para la **transición** de la entidad de **IPv4 a IPv6**. Documentar el Plan de diagnóstico para la transición de IPv4 a IPv6.

9.3. FASE DE IMPLEMENTACIÓN:

Metas	Actividades \ Instrumentos \ Resultados
Establecer el Plan de implementación de seguridad de la información	**Implementar** el **plan de implementación** del **modelo de seguridad y privacidad** de la información el cual debe ser revisado y aprobado por el comité de riesgos
Ejecutar el plan de tratamiento de riesgos	**Ejecutar** el **plan de tratamiento de los riesgos** transversales de seguridad de la información identificados en la fase de planificación que fue presentado en el comité de riegos.
Ejecutar del plan y estrategia	**Ejecutar plan de transición a IPv6** y elaborar informe de

de transición de IPv4 a IPv6.	implementación.
Establecer Indicadores De gestión de seguridad	**Definir los indicadores** para medir la gestión del modelo de seguridad y establecer los mecanismos para su medición. Estos indicadores deben permitir verificar la eficacia y efectividad de los controles implementados para mitigar los riesgos de seguridad de la entidad.
Implementar procedimiento de Gestión de Eventos e incidentes de seguridad	**Implementar** el procedimiento y los mecanismos para la **gestión de los eventos e incidentes de seguridad** de la información**.**
Implementar procedimiento de gestión de vulnerabilidades	**Implementar** el procedimiento y los mecanismos para la **gestión de vulnerabilidades seguridad** de la información**.**
Ejecutar plan de capacitación y sensibilización de seguridad	**Ejecutar** el plan anual de capacitación, socialización y sensibilización de seguridad de la información
Ejecutar pruebas anuales De vulnerabilidades e intrusión	**Ejecutar** el plan anual de **pruebas vulnerabilidades** e intrusión con el objetivo de identificar el nivel de protección de los activos de información de la entidad. Para tal efecto, se deberá tener en cuenta los respectivos requerimientos de seguridad relacionados con pruebas de vulnerabilidades establecidos en la circular externa 029 de 2014 de la Superfinanciera de Colombia o la circular que las reemplacen.
Ejecutar pruebas de Ethical Hacking	**Ejecutar** pruebas anuales de **Ethical Hacking** orientadas a poder determinar los niveles de riesgo y exposición de la organización ante atacantes interno o externo que puedan a comprometer activos críticos de la entidad y con esto generar interrupción en los servicios, afectar la continuidad del negocio y/o acceder de forma no autorizada a la información sensible o clasificada de la entidad o de carácter personal de los trabajadores o terceros que laboren para la entidad.
Ejecutar pruebas de Ingeniera Social	**Ejecutar** pruebas anuales de **ingeniería social** orientadas a verificar aspectos como: (i) los protocoles internos de seguridad, (ii) el nivel de concientización de los funcionarios y terceros que laboren en la entidad sobre temas de seguridad de la información, (iii) el conocimiento y/o cumplimiento de las políticas de seguridad y privacidad de la información de la entidad y (iv) el nivel de exposición de la información publicada en internet de la entidad y

	de sus empleados.

9.4. FASE DE EVALUACIÓN:

Metas	Actividades \ Instrumentos \ Resultados
Ejecución De auditorías de seguridad de la información	**Ejecución de auditorías** del modelo de seguridad y de temas normativos y de cumplimiento de seguridad de la información aplicables a la entidad, de acuerdo con el plan de auditoria revisado y aprobado por la Alta Dirección. Las auditorías internas se deberán llevar a cabo para la revisión del Sistema de Gestión de Seguridad 'SGSI' de la Información implementado en la entidad, con la finalidad de verificar que los objetivos de control, controles, procesos y procedimientos del SGSI cumpla con los requisitos establecidos en la norma ISO 27002:2015 y los del MSPI.
Plan De seguimiento, evaluación y análisis de SGSI	**Elaboración documento** con el **plan de seguimiento, evaluación y análisis del SGSI** revisado y aprobado por el Comité de Riesgos.

9.5. FASE DE MEJORA CONTINUA

Metas	Actividades \ Instrumentos \ Resultados
Diseñar plan de mejoramiento	**Diseñar** el **plan de mejoramiento continuo de seguridad** y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el Sistema de Gestión de Seguridad de la Información.

Fuentes: Modelo de Seguridad y privacidad de la información MINTIC
Plan de seguridad y privacidad de la información Findeter

10. SITUACIÓN ACTUAL.

Política de Seguridad y privacidad de la información

El Fondo de Pasivo social de Ferrocarriles nacionales de Colombia, adopto las políticas de Seguridad de la Información, por medio por medio de la resolución 0846 de junio 9 de 2017, donde se determinan los

lineamientos que permiten proteger los activos de la entidad mediante mecanismo de aseguramiento que permitan el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y no repudio.

Activos de información

La entidad cuenta con el inventario de activos de información que fue actualizado por última vez en el año 2016 y con un procedimiento donde se indican las actividades que se deben tener en cuenta para su actualización, pero no se cuenta con una guía donde se indiquen los lineamientos para la identificación, valoración y clasificación de los activos de información, así como la verificación y seguimiento del cumplimiento del tratamiento de la información.

Programa concienciación en seguridad y privacidad de la información del sistema de gestión de la seguridad y la información

En el 2017 el proceso de gestión de TIC´s creó el programa concienciación en seguridad y privacidad de la información del sistema de gestión de la seguridad la información donde se establecieron las actividades y fases que se deben llevar a cabo para la toma de conciencia en seguridad de la información para los funcionarios y/o contratista.

Elaboración de Matriz de Riesgo de Seguridad de la Información

Durante el año 2018 se realizó el levantamiento de riesgo de seguridad la información para los 14 procesos de la entidad conforme a la metodología de administración de riesgo del fondo, obteniendo 11 riesgos que fueron aprobados en comité de Gestión y Desempeño mediante acta No 005 del 27 de julio de 2018.

Protección de Datos Personales

Se documentó el MANUAL DE POLÍTICAS DE TRATAMIENTO DE DATOS PERSONALES, donde se establecieron las políticas de control para garantizar la protección de datos personales recolectados, recibidos y transmitidos de parte de funcionarios, contratistas, pensionados, afiliados y beneficiarios, dando cumplimiento a lo establecido en el Artículo 17 literal k de la Ley 1581 de 2012 por medio de la cual se dictan disposiciones generales para la protección de esta información, y el Decreto 1377 de 2013 que reglamenta parcialmente la Ley 1581 de 2012 por medio del proceso de asistencia jurídica.

Modelo de Seguridad y Privacidad de la Información. Durante el 2019 se realizó evaluación a la implementación del modelo de seguridad y privacidad de la información del Mintic – MSPI mediante la herramienta instrumento de evaluación MSPI donde se obtuvo el 48% de la efectividad de los controles y el

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	96	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	64	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	66	100	GESTIONADO
A.9	CONTROL DE ACCESO	59	100	EFECTIVO
A.10	CRIPTOGRAFÍA	20	100	INICIAL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	44	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	40	100	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	31	100	REPETIBLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	16	100	INICIAL
A.15	RELACIONES CON LOS PROVEEDORES	40	100	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	14	100	INICIAL
A.18	CUMPLIMIENTO	56	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		48	100	EFECTIVO

54% en el avance ciclo de funcionamiento del modelo de operación (PHVA) como se aprecia a continuación:

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2015	Planificación	31%	40%
2016	Implementación	10%	20%
2017	Evaluación de desempeño	5%	20%
2018	Mejora continua	8%	20%
TOTAL		54%	100%

11. ACTIVIDADES

Teniendo en cuenta la política de seguridad y privacidad adoptada por la entidad y el diagnostico obtenido a través del instrumento de evaluación de la implementación del modelo de seguridad y privacidad de la información suministrado por el MINTIC, El Fondo de Pasivo Social ferrocarriles Nacionales de Colombia establece el plan para la implementación del modelo de Seguridad y Privacidad de la Información a través del FORMATO PLAN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (APGTSOPSF014), con las siguientes actividades:

- Determinar el estado actual de la gestión de seguridad de la entidad
- Documento de Declaración de aplicabilidad
- Guía de identificación y clasificación de activos de información.
- Levantamiento de activos de información
- Publicación de Activos de Información
- Índice de información clasificada y reservada
- Inventario de Bases de Datos Pesonales
- Realizar el Registro de Base de Datos Personales
- Realizar la identificación y valoración de los riesgos transversales de seguridad de la información y seguridad digital.
- Aceptación de Riesgos Identificados de seguridad de la información y seguridad digital
- Publicación de Matriz de riesgos de seguridad de la información
- Implementación y seguimiento del plan de tratamiento de riesgos de seguridad y privacidad de la información.
- Creación del procedimiento para la gestión de incidentes.
- Socializar el procedimiento de gestión de incidentes
- Diseño e Implementación controles de Anexo A ISO 27001:2013
- Plan de Sensibilización en seguridad y privacidad de la información
- Plan de infraestructuras críticas del Sector
- Plan de diagnóstico IPV4 a IPV6
- Implementación del plan de transición de IPV4 a IPV6
- Actualización del firewall
- Plan de continuidad del negocio
- Redefinición de roles y responsabilidades
- Integración del MSPI con el sistema de gestión documental de la entidad
- Alinear los riesgos identificados en seguridad de la información y seguridad digital a la metodología adoptada por la entidad
- Definición de Indicadores de Gestión
- Implementación del plan de sensibilización y seguridad de la información

- plan de tratamiento de datos personales
- Implementación y seguimiento del plan de tratamiento de datos personales
- Diseño de pruebas
- Realización de Pruebas y Análisis de vulnerabilidad
- Auditoria interno
- Diseñar el plan de mejoramiento

Ver anexo. FORMATO PLAN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (APGTSOPSF014).

12. PASOS PARA LA FORMULACION SEGUIMIENTO Y VERIFICACION DEL PLAN DE SEGURIDAD.

Responsable	Actividad
Encargado de seguridad de la información / Oficina Asesora de Planeación y Sistemas	Actualizar la herramienta instrumento de evaluación MSPI del MICTIC, entre el (1) primero del mes de octubre y 30 del mes de noviembre de cada vigencia.
Encargado de seguridad de la información / Oficina Asesora de Planeación y Sistemas	Definir las actividades del Plan de seguridad y privacidad de la información en el formato APGTSOPSF014, teniendo en cuenta el nivel de madurez identificado en el instrumento de evaluación del MINTIC
Encargado de seguridad de la información / Oficina Asesora de Planeación Y Sistemas	Presentar el Plan de seguridad y privacidad de la información en el formato APGTSOPSF014 al jefe de la Oficina Asesora de Planeación para su VoBo el 16 día hábil del mes diciembre de cada vigencia.
Encargado de seguridad de la información/ Jefe Oficina Asesora de Planeación y Sistemas.	Presentar diligenciado FORMATO PLAN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (APGTSOPSF014) de la vigencia al COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO para su evaluación y aprobación.
Encargado de seguridad de la información/ Jefe Oficina Asesora de Planeación y Sistemas.	Enviar PLAN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN y diligenciado el FORMATO PLAN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (APGTSOPSF014) y aprobado por el comité, al administrador de la página Web, para su publicación en la página de la entidad a más tardar el treinta y uno (31) de enero de cada año.

Encargado de seguridad de la información/ Jefe Oficina Asesora de Planeación y Sistemas.	Enviar mediante correo electrónico; diligenciado FORMATO PLAN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (APGTSOPSF014) al Jefe de la Oficina de Control Interno y/o quien haga sus veces para su verificación y seguimiento, el quinto (5) día hábil del mes de mayo y (5) día hábil del mes de Octubre de cada vigencia.
Auditores de Control Interno /Jefe De La Oficina De Control Interno Y/O Quien Haga Sus Veces	Recibir el quinto (5) día hábil siguiente al vencimiento del diligenciado FORMATO PLAN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (APGTSOPSF014) realizar el seguimiento semestral y solicitar a los funcionarios responsables del producto planeado, los soportes que sustentan el avance reportado.