FONDO DE PASIVO SOCIAL
FERROCARRILES NACIONALES DE COLOMBIA

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Fecha de Vigencia: 26/12/2020

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	**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

La administración de riesgos es un componente estratégico que le permite a la alta Dirección, a través del análisis del entorno que rodea a la Entidad a nivel interno y externo, la identificación, medición, control y monitoreo de posibles eventos que pueden afectar la consecución de los objetivos trazados.

2. OBJETIVO

Definir la metodología de gestión de riesgo de seguridad de la información que permita identificar, medir, controlar, monitorear y comunicar los riesgos de seguridad asociados a cada uno de los proceso del Fondo de Pasivo Social Ferrocarriles Nacionales de Colombia que puedan afectar el cumplimiento de objetivos misionales y estratégicos.

3. ALCANCE

La Guía Metodológica de Análisis de Riesgos de Seguridad de la Información será aplicada por los funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con el Fondo de Pasivo Social Ferrocarriles Nacionales de Colombia; dicho tratamiento de riesgo debe involucrar a todos los procesos y actividades desarrolladas por la Entidad, en especial aquellos que impactan directamente la consecución de los objetivos misionales.

4. BASES LEGALES

- **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.

- **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 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.

- **Norma Técnica Colombiana NTC- ISO 31000:2015** Gestión del Riesgo. Principios y directrices.

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

- **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.

5. DEFINICIONES

Activo de información: aquello que es de alta validez y que contiene información vital de la empresa que debe ser protegida.

Amenaza: Es la causa potencial de un daño a un activo de información.

Análisis de riesgos: Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos. Causa: Razón por la cual el riesgo sucede.

Confidencialidad: Propiedad que determina que la información no esté disponible a personas no autorizados

Controles: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.

Disponibilidad: Propiedad de determina que la información sea accesible y utilizable por aquellas personas debidamente autorizadas.

Dueño del riesgo sobre el activo: Persona responsable de gestionar el riesgo.

Impacto: Consecuencias de que la amenaza ocurra. Nivel de afectación en el activo de información que se genera al existir el riesgo.

Incidente de seguridad de la información: Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Oficial de Seguridad: Persona encargada de administrar, implementar, actualizar y monitorear el Sistema de Gestión de Seguridad de la Información.

Probabilidad de ocurrencia: Posibilidad de que se presente una situación o evento específico.

Responsables del Activo: Personas responsables del activo de información.

Riesgo: Grado de exposición de un activo que permite la materialización de una amenaza.

Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Riesgo Residual: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo.

Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información (ISO 27000:2014).

SGSI: Siglas del Sistema de Gestión de Seguridad de la Información.

Sistema de Gestión de Seguridad de la información SGSI: permite establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma NTC-ISO-IEC 27001.

Vulnerabilidad: Debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad de caracteriza por ausencia en controles de seguridad que permite ser explotada.

6. METODOLOGIA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Para la metodología de evaluación y tratamiento el Fondo de Pasivo Social Ferrocarriles Nacionales de Colombia se basa en el Proceso para la administración del riesgo en seguridad de la información de la ISO 27005

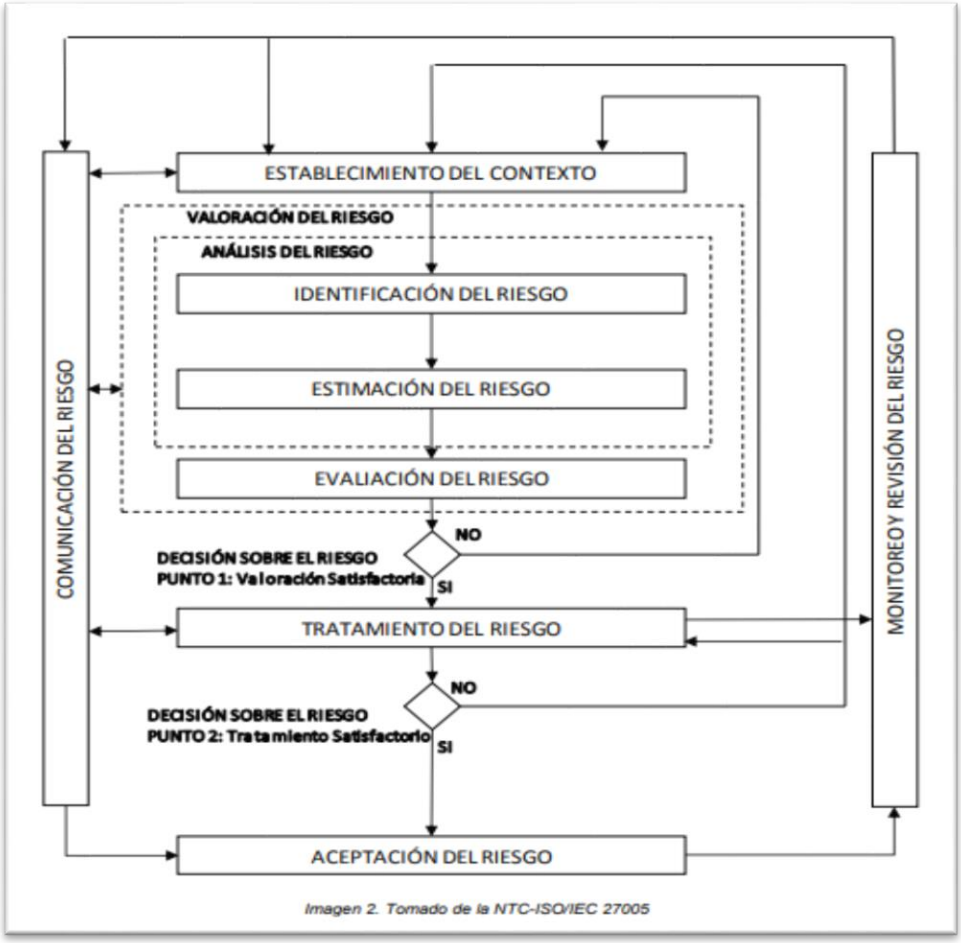


Imagen 2. Tomado de la NTC-ISO/IEC 27005

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.

7. ESTABLECIMIENTO DE CONTEXTO

En esta fase los propietarios de los procesos deben definir los parámetros internos y externos que se toman a consideración para la gestión del riesgo en seguridad de la información y la definición del alcance, límites y la política del SGSI, con el fin de asegurar que todos los activos de información de la entidad se contemplen en el SGSI, mediante el establecimiento de los criterios básicos tales como: criterios de evaluación del riesgo, criterios de impacto, criterio de aceptación del riesgo.

8. ETAPAS PARA LA GESTION DE RIESGOS.

Para la gestión del riesgo se establecen las siguientes etapas:

8.1. IDENTIFICACION

La identificación del riesgo se hace con base en causas identificadas para los procesos, dichas causas pueden ser internas o externas, según lo que haya identificado la Entidad a través del Contexto estratégico.

El propósito de la identificación del riesgo es determinar que podría suceder que cause una perdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir una perdida

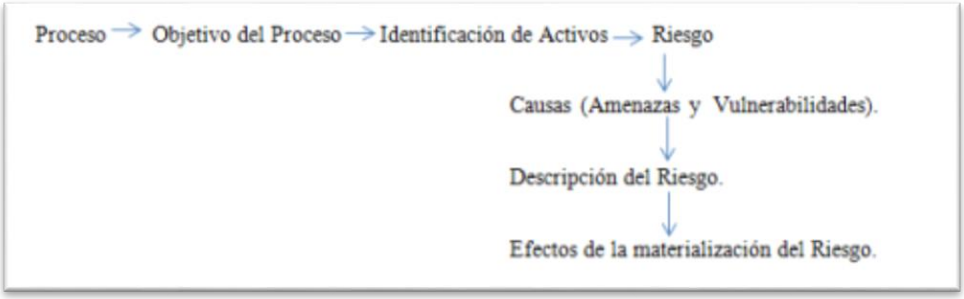
Es importante establecer cuáles son los activos críticos para asociarlos a los procesos correspondientes y de allí generar el listado de procesos críticos. Inventariar los activos de información sensible, revisar los procesos según la clasificación del MECI y del modelo de gestión, con éste punto se revisa la pertinencia del alcance planteado para el MSPI[1].

8.2. VALORACIÓN DE LOS RIESGOS

En esta etapa se genera una lista completa de los riesgos sobre la base de los acontecimientos que puedan crear, mejorar, prevenir, degradar, acelerar o retrasar la consecución de los objetivos del

[1] Guía del Gestión de riesgos https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

FPS-FNC. Las debilidades de los procesos en cuanto a seguridad de la información, los riesgos a los cuales se encuentran expuestos y las causas que podrían comprometer la confidencialidad, integridad y disponibilidad de los procesos deben ser identificadas y evaluadas teniendo en cuenta los criterios de evaluación definidos. En este proceso se debe realizar las siguientes actividades: Identificar el flujo de información de cada uno de los procesos, Identificar las vulnerabilidades que existen en el proceso, Identificar las amenazas que podrían materializarse, dadas las vulnerabilidades existentes y definir las escalas a utilizar



2

Para cada riesgo, se deben analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

8.3. ANÁLISIS DEL RIESGO

El objetivo del Análisis de Riesgos es identificar y valorar los riesgos a los cuales están expuestos los procesos y los flujos de información, para identificar y seleccionar los controles apropiados de seguridad. El análisis está basado en los flujos de información de cada uno de los procesos y los requerimientos de seguridad, tomando en cuenta los controles existentes.

En esta etapa se definen los criterios que se deben utilizar para evaluar la importancia del riesgo,

[2] https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

para los cuales la entidad establece las siguientes métricas de calificación por Probabilidad e impacto definiendo 5 niveles de medición

PROBABILIDAD:

se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de Frecuencia, si se ha materializado (por ejemplo: número de veces en un tiempo determinado), o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado.

TABLA DE PROBABILIDAD			
NIVEL	**DESCRIPTOR**	**DESCRIPCIÓN (FACTIBILIDAD)**	**FRECUENCIA**
1	**RARO**	Puede que el riesgo no se haya presentado, o que ocurra solo en circunstancias excepcionales.	Nunca o no se ha presentado en los últimos 5 años
2	**IMPROBABLE**	El riesgo pudo ocurrir en algún momento, es poco común o frecuente	Al menos de 1 vez en los últimos 5 años.
3	**POSIBLE**	El riesgo puede ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años.
4	**PROBABLE**	El riesgo ocurrirá en la mayoría de las circunstacias.	Al menos de 1 vez en el último año.
5	**CASI SEGURO**	Se espera que el riesgo ocurra en la mayoria de las circunstancias.	Más de 1 vez al año.

IMPACTO

Se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo

TABLA DE IMPACTO		
NIVEL	**DESCRIPTOR**	**DESCRIPCIÓN**
1	INSIGNIFICANTE	**Si el hecho llegara a presentarse, tendría consecuencias o efectos MÍNIMOS** sobre el proceso y/o la entidad.
2	MENOR	**Si el hecho llegara a presentarse, tendría BAJAS** consecuencias o efectos sobre el proceso y/o la entidad.
3	MODERADO	**Si el hecho llegara a presentarse, tendría MEDIANAS** consecuencias o efectos sobre el proceso y/o la entidad.
4	MAYOR	**Si el hecho llegara a presentarse, tendría ALTAS** consecuencias o efectos sobre el proceso y/o la entidad.
5	CATASTRÓFICO	**Si el hecho llegara a presentarse, tendría DESASTROSAS** consecuencias o efectos sobre el proceso y/o la entidad.

De esta forma se procede a hacer la “calificación del riesgo”, en la cual se realiza una estimación, de cuál podría ser la probabilidad de ocurrencia del riesgo y el impacto que traería éste, en caso de materializarse.

La calificación, se hace de manera cualitativa generando una comparación en la cual se presenta el análisis de la probabilidad de ocurrencia del riesgo versus el impacto del mismo, obteniendo al final la matriz denominada “Matriz de Calificación, Evaluación y respuesta a los Riesgos”, con la cual la guía presenta la forma de calificar los riesgos con los niveles de impacto y probabilidad establecidos anteriormente, así como las zonas de riesgo presentando la posibles formas de tratamiento que se le puede dar a ese riesgo, tal como se muestra en la siguiente imagen:

Matriz de Calificación, Evaluación y respuesta a los Riesgos

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo *Moderada*: Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo *Alta*: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo *Extrema*: Reducir el riesgo, Evitar, Compartir o Transferir

Fuente: Guía de Riesgos DAFP

8.4. EVALUACIÓN DE LOS CONTROLES ESTABLECIDOS PARA LA MITIGACIÓN DE LOS RIESGOS.

La Evaluación de los controles se realiza cuando se ha establecido el riesgo inherente para los procesos y el impacto y probabilidad de ocurrencia de cada uno de los riesgos establecidos.

Los controles deben estar documentados de forma tal que es posible conocer cómo se lleva a cabo el control, quién es el responsable de su ejecución y cuál es la periodicidad para su ejecución, lo cual determinará las evidencias que van a respaldar la ejecución del mismo.

8.5. NIVELES DE RIESGO.

Con base al resultado del análisis de riesgo es posible establecer la severidad de estos, para los cuales se determinan 4 zonas de riesgos en el mapa, que permite al Líder del Proceso priorizarlos y determinar sobre los cuales se debe tener mayor control, proponiendo acciones de mejora que propenden conservar las características de confidencialidad, integridad y disponibilidad de la información.

B: Zona de riesgo Baja
M: Zona riesgo Moderada
A: Zona de riesgo Alta
E: Zona de riesgo Extrema

8.6. TRATAMIENTO DE RIESGOS

Para cada zona de riesgo la entidad establece las siguientes opciones de manejo del riesgo:

ZONA DE RIESGO	OPCIONES DE MANEJO DEL RIESGO	
BAJA	* Asumir el riesgo	Se asume el riesgo. **Nota:** Si el riesgo inherente se ubica en la zona baja, se debe revisar si éste riesgo amerita o no, que se incluya en el mapa de riesgos, para su administración.
MODERADA	* Asumir el riesgo * Reducir el riesgo	Se asume el riesgo. Se implementan ***controles*** *y* sus ***acciones de manejo del riesgo*** orientadas a **disminuir** la probabilidad de materialización del riesgo Y/O ***controles*** y sus ***acciones de manejo del riesgo*** , orientadas a **disminuir** el impacto de la materialización del riesgo. Lo anterior con el propósito de llevar el riesgo a la zona baja.
ALTA	* Reducir el riesgo * Evitar el riesgo * Compartir o transferir el riesgo	Se implementan ***controles*** *y* sus ***acciones de manejo del riesgo,*** orientadas *a* **disminuir** o **evitar** la materialización del riesgo Y/O ***controles*** y sus ***acciones de manejo del riesgo*** orientadas *a* **disminuir** **o** **evitar** el impacto de la materialización del riesgo. Lo anterior con el propósito de llevar el riesgo a zona moderada. En lo relacionado con compartir o transferir el riesgo, se podría establecer el mantenimiento de pólizas (contratos de seguros), tercerización, entre otras; como controles o acciones de manejo del riesgo enfocadas a la protección. Esta opción de manejo se deberá tener en cuenta, con base en la capacidad del proceso y/o la entidad, para asumir las consecuencias del impacto producido por la materialización del riesgo.
EXTREMA	* Reducir el riesgo * Evitar el riesgo * Compartir o transferir el riesgo	Se implementan ***controles*** y sus ***acciones de manejo del riesgo*** , orientadas a **disminuir** o **evitar** la materialización del riesgo Y/O ***controles*** y sus ***acciones de manejo del riesgo*** orientadas a **disminuir** o **evitar** el impacto de la materialización del riesgo. En lo relacionado con **Compartir o transferir el riesgo**, teniendo en cuenta que en esta zona de riesgo se pueden producir pérdidas considerables para el proceso y/o la entidad, se hace necesario que se implementen **controles** de protección y sus **acciones de manejo del riesgo,** en los cuales se involucren

OPCIONES DE MANEJO DEL RIESGO

ASUMIR EL RIESGO: Implica que se ACEPTAN las consecuencias o efectos de la materialización del riesgo; en este caso no es necesario tomar medidas para seguir disminuyendo la probabilidad e impacto del riesgo.

REDUCIR EL RIESGO: Implica tomar medidas encaminadas a DISMINUIR tanto la PROBABILIDAD, como el IMPACTO. La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Por ejemplo: a través

de la mejora u optimización de los procedimientos, la implementación de acertados controles y acciones de manejo complementarias.

EVITAR EL RIESGO: Implica tomar medidas encaminadas a PREVENIR que el riesgo se materialice, evitar la materialización del riesgo es la primera alternativa a considerar, y esto se logra cuando al interior del proceso se generan CAMBIOS SUSTANCIALES, tales como: mejoramiento a raiz de ajustes drásticos, rediseños o eliminaciones realizados en procedimientos u otros controles establecidos. Por ejemplo: el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.

COMPARTIR O TRANSFERIR EL RIESGO: Implica tomar medidas que REDUZCAN EL IMPACTO de la materialización del riesgo, a través del COMPARTIR O TRASPASO de las pérdidas potenciales a otras organizaciones o entidades, como en el caso de los contratos de seguros (Pólizas) o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Por ejemplo, tercerización (Outsourcing), la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar.

8.7. SEGUIMIENTO Y REVISIÓN DEL PROCESO DE GESTIÓN DE RIESGOS

El monitoreo y revisión es una fase que permite asegurar que las acciones y controles que se han implementado son eficientes y para evidenciar todas aquellas situaciones que pueden intervenir en las aplicaciones de acciones preventivas.

El monitoreo debe estar a cargo de los dueños de los procesos, la oficina de control interno y el oficial de seguridad, aplicando y sugiriendo los correctivos y ajustes necesarios para propender por un efectivo manejo del riesgo

Dentro de las actividades que se ejecutan en esta fase, se tienen:

• Analizar los cambios, las tendencias, los éxitos y los fracasos dentro del proceso de gestión de riesgos de seguridad de la información.

• Detectar cambios en el contexto interno o externo, incluyendo los cambios que se puedan presentar en los criterios de riesgos de seguridad de la información.

• Revisar la implementación de los planes de tratamiento de riesgo de seguridad de la información y las prioridades de implementación de estos.

• Identificación de nuevos riesgos de seguridad de la información.

• La revisión de la gestión de riesgos se debe hacer por lo menos una vez al año, el seguimiento a los riesgos debe ser permanente por parte de los líderes de los procesos.

9. BIBLIOGRAFÍA

Guía para la Administración del Riesgo del Departamento Administrativo de la Función Pública (DAFP).
https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+Públicas+-+Guía+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b

Guía de gestión de riesgos-MINTIC

https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf