DISEÑO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN BASADA EN LOS REQUERIMIENTOS DE LA ESTRATEGIA DE GOBIERNO EN LÍNEA PARA LA ENTIDAD EL FONDO PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA

ROSELYS SILVA CUADRADO
HENRY JARA VELANDIA

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2017

DISEÑO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN BASADA EN LOS REQUERIMIENTOS DE LA ESTRATEGIA DE GOBIERNO EN LÍNEA PARA LA ENTIDAD EL FONDO PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA

ROSELYS SILVA CUADRADO
HENRY JARA VELANDIA

Proyecto de grado para optar el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Asesor
JUAN CARLOS ALARCÓN
Ingeniero de sistemas

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2017

NOTA DE ACEPTACIÓN

_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá, Enero de 2017

DEDICATORIA

Esta dedicatoria es para Dios, que nos da la vida, la fuerza, la sabiduría, la motivación y el empeño para salir adelante, que nos pone pruebas difíciles pero no imposibles, que nos enseña que la diferencia entre el fracaso y el éxito radica en la fe y la voluntad que le ponemos a las cosas.

Sin la fuerza que él nos coloca en el alma, no hay actividad, labor o proyecto de vida que se pueda realizar y llevar a feliz término, gracias Dios por permitirnos culminar con esta tesis, un eslabón más en la escalera que significa la vida profesional, e incluso en la vida personal, porque no solo aprendimos a ser especialistas en seguridad de la información sino también a ser mejores personas.

AGRADECIMIENTO

En agradecimiento primero que todo a Dios, quien nos permite vivir y tener las capacidades necesarias para cumplir con nuestros sueños.

A nuestras familias que siempre han sido un apoyo en esta constante, difícil y gratificante profesión como ingenieros.

A nuestros docentes de la especialización cuyo profesionalismo y buen trato fue fundamental para adquirir el conocimiento con el que ahora contamos, especialmente al ingeniero Juan Carlos Alarcón, asesor de nuestra tesis ya que con su apoyo, criterio y respeto, nos guió por el camino indicado para llevar a buen término este proyecto.

A la entidad Fondo de Pasivo Social Ferrocarriles Nacionales de Colombia, encabezada por el Dr. Mauricio Villaneda, jefe de la oficina asesora de planeación y sistemas que junto con su equipo de trabajo siempre estuvieron dispuestos a prestarnos su acompañamiento y apoyo durante la realización de esta tesis.

A todas aquellas personas que nos prestaron su apoyo para la elaboración de este proyecto, ya fuese de manera intelectual o moral.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE CUADROS

pág.

INTRODUCCIÓN

El presente proyecto de grado se elabora en base a la estrategia de Gobierno en Línea y plantea el diseño de un plan de seguridad y privacidad de la información para la entidad Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia, teniendo en cuenta como marco de referencia la norma ISO 27001-2013, para de esta manera brindar a la entidad una herramienta que le permita cumplir con su aspiración de ser parte de las entidades que mediante las TIC buscan contribuir a que el Estado sea un ente más eficiente, transparente y participativo.

La característica principal del diseño del plan de seguridad y privacidad de la información, radica en que se manejan estrategias como Gobierno en Línea pero sobretodo se utilizan conceptos y conocimientos adquiridos durante la especialización en Seguridad Informática cursada en la Universidad Piloto de Colombia en materias tales como Gestión de la Seguridad, seguridad operativa, investigación I y II entre otras.

Por otra parte, se tiene en cuenta que la entidad Fondo de Pasivo Social de Ferrocarriles de Colombia no cuenta con un modelo ni un plan de Seguridad y Privacidad de la Información, lo que le permitiría garantizar que los riesgos sean conocidos, asumidos, gestionados y minimizados, adicional a esto, el proceso Gestión TIC´S ha mostrado su interés y ha tomado la decisión de iniciar el proceso de implementación del eje temático trasversal de la estrategia de Gobierno en Línea, enmarcado en un “Diseño del Modelo de Seguridad y Privacidad de la Información” , motivo por el cual, el plan de seguridad propuesto en este documento, es un insumo importante para lograr dicho objetivo.

A continuación se describe en detalle el proyecto.

1. PROBLEMA

1.1 FORMULACIÓN DEL PROBLEMA

El gobierno se encuentra en aras de lograr un estado eficiente, más trasparente y preocupado en la seguridad y privacidad de los datos de los ciudadanos que garantice la interoperabilidad entre entidades, servicios e información en línea, integral, con calidad, y donde el ciudadano sienta al gobierno como un ente de confianza, de gestión trasparente, eficiente, eficaz y disponible al público.

Por ello es conveniente que dentro de las entidades trabajen mancomunadamente en la protección del activo más importante que es su información, frente a las amenazas informáticas a las que están expuestas en el mundo de hoy, mediante una evaluación de riesgos y una medición de la eficacia de los mismos.

Un Modelo de Seguridad y Privacidad de la Información reúne el conjunto de lineamientos, políticas, normas, procesos e instituciones que proveen y promueven la puesta en marcha, supervisión, mejora y control de la implementación del modelo, así como a la implementación de la Estrategia de Gobierno en Línea o gobierno electrónico[1].

En el Fondo Pasivo Social Ferrocarriles Nacionales de Colombia existe una problemática detectada, y es que al ser una entidad del estado del Orden nacional debe cumplir con el Decreto 1078 de 2015. (Pág. 138 y 139), que define los lineamientos, instrumentos y plazos de la estrategia de Gobierno en Línea, dividida en cuatro subcategorías: TIC para el Gobierno abierto, TIC para servicios, TIC para la gestión y Seguridad y privacidad de la información.

El problema radica en que EL Fondo de Pasivo Social Ferrocarriles Nacionales de Colombia no gestiona de manera apropiada los riesgos de seguridad de la información que enfrenta, sumado al hecho de que no se está cumpliendo con las

[1]Modelo de Seguridad y Privacidad de la Información [en línea]. Bogotá D.C.: Ministerio de Tecnologías de la Información y las Comunicaciones, 2015 [consultado 02 de Octubre de 2015]. Disponible en Internet pág. 9

directrices del decreto de la estrategia de Gobierno En Línea (GEL).Por ello se plantea un diseño de modelo de seguridad y privacidad como posible herramienta para que los riesgos sean conocidos, asumidos, gestionados y minimizados por la entidad de una forma documentada, sistemática, estructurada y adaptada a los cambios que se produzcan en el entorno y las tecnologías y que existan políticas y procedimientos encaminados a la búsqueda del cumplimiento de las directrices de la estrategia de gobierno en línea.

1.2 PREGUNTA PROBLEMA

¿Cómo El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia puede asegurar de forma efectiva la información que genera y utiliza en sus procesos misionales y dar cumplimiento al componente de seguridad de la información de la estrategia de Gobierno en Línea?

1.3 JUSTIFICACIÓN

Teniendo en cuenta la estrategia de gobierno en línea, nombre que recibe la estrategia de gobierno electrónico (e-government) en Colombia, y que busca contribuir un Estado más eficiente, transparente y participativo gracias al uso de las Tecnologías de Información y Comunicación, mediante mejores servicios en línea al ciudadano, mejorando la gestión de las diferentes entidades del gobierno, lo que a su vez generará confianza en los ciudadanos e impulsará y facilitará las acciones para avanzar en los objetivos del desarrollo sostenible y el goce efectivo de los derechos a través de TIC.

El Fondo Pasivo Social Ferrocarriles Nacionales de Colombia, más puntalmente el área de Gestión de TIC ha tomado la decisión de iniciar el proceso de implementar el eje temático 4 de la estrategia de Gobierno en Línea, definido como el “Diseño del Modelo de Seguridad y Privacidad de la Información”, para lo cual ha escogido la norma ISO/IEC 27001:2013.

En el marco de lo antes mencionado, como estudiantes de especialización de Seguridad Informática, y en vista de que la línea temática “Gestión de la Seguridad y el Riesgo” está dentro de las opciones para realizar el proyecto de grado, se decidió optar por unificar ambas situaciones y desarrollar el proyecto de grado, mediante la vinculación como líderes del proceso de Diseño del modelo de

seguridad y privacidad de la Información del Fondo de Pasivo Social Ferrocarriles Nacionales de Colombia.

1.4 OBJETIVOS

1.4.1 Objetivo general. Diseñar un plan de seguridad y privacidad de la información empleando la estrategia de gobierno en línea para el Fondo Pasivo Social Ferrocarriles Nacionales de Colombia.

1.4.2 Objetivos específicos. Se identificaron los siguientes:

- Realizar un diagnóstico de la situación actual del Fondo Pasivo Social Ferrocarriles Nacionales de Colombia en relación con los requerimientos de la estrategia de gobierno en línea en el componente de seguridad y privacidad de la información.

- Identificar y realizar el inventario de activos de información.

- Identificar vulnerabilidades y amenazas de seguridad de la información.

- Definir la metodológica para agestión de riesgo de seguridad de la información.

- Definir el alcance y los objetivos del modelo de seguridad y privacidad de la información.

- Diseñar una política de seguridad y privacidad de la información que sea desplegada a los funcionarios del Fondo Pasivo Social Ferrocarriles Nacionales De Colombia.

1.5 TIPO DE INVESTIGACIÓN

El diseño metodológico que se utilizará para la realización de este proyecto es un estudio descriptivo.

1.6 HIPÓTESIS

Hi: El diseño de un plan de seguridad y privacidad de la información permite a la entidad Fondo de Pasivo Social Ferrocarriles Nacionales de Colombia cumplir con lo requerido en la estrategia de gobierno en línea cuyo propósito es brindar un estado más eficiente, transparente y participativo.

Ho: La no realización del diseño de un plan de seguridad y privacidad de la información llevará a la entidad Fondo de Pasivo Social Ferrocarriles Nacionales de Colombia a no cumplir con lo requerido en la estrategia de gobierno en línea cuyo propósito es brindar un estado más eficiente, transparente y participativo.

1.7 VARIABLES

1.7.1 Variable independiente o explicativa. Diseño del modelo de seguridad y privacidad de la información.

1.7.2 Variable dependiente o explicada. Requerimiento de la estrategia de gobierno en línea.

2. MARCO REFERENCIAL

2.1 DESCRIPCIÓN DE LA COMPAÑIA

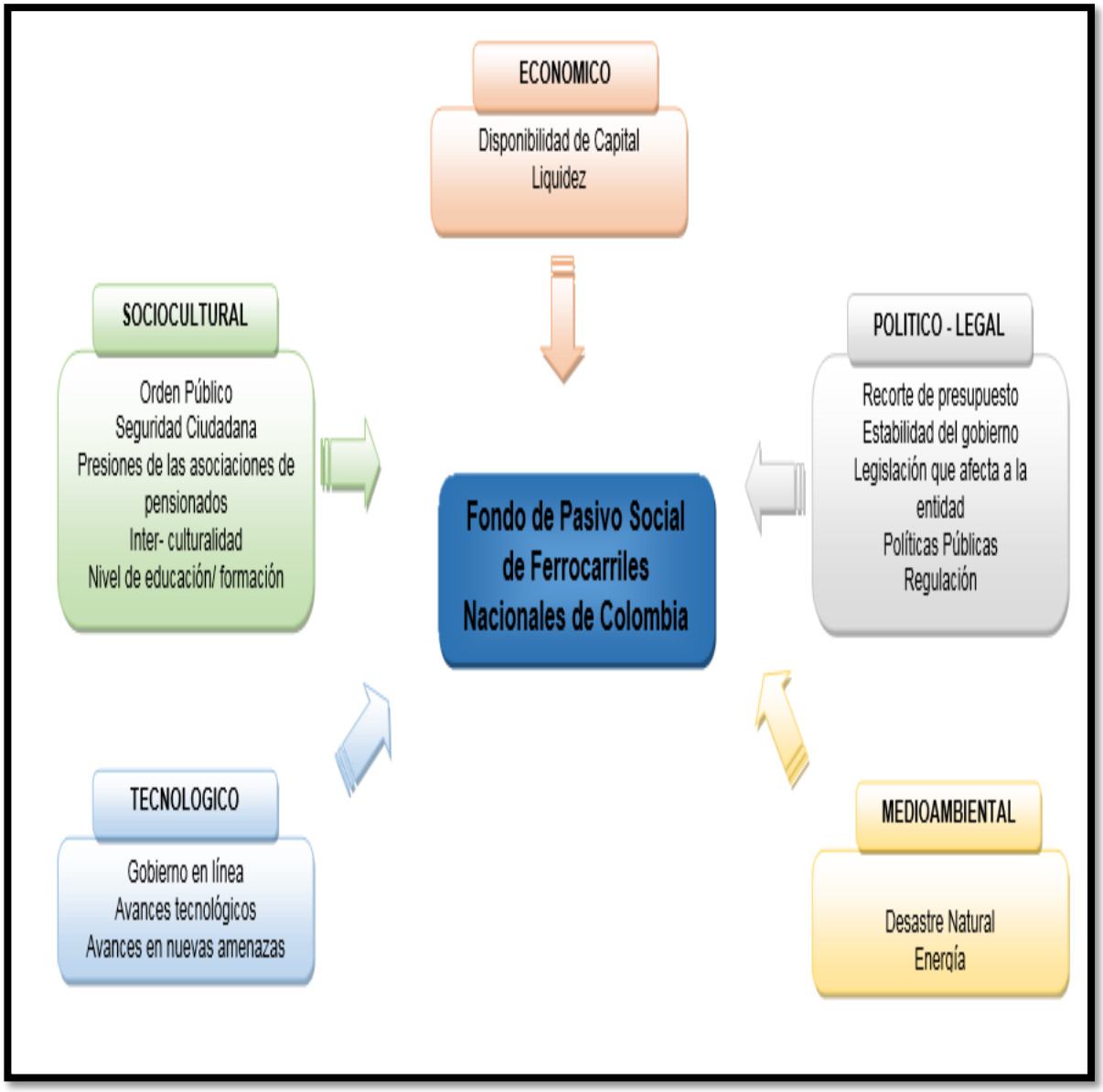
El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia, es una Empresa del sector público adscrita al Ministerio de la Protección Social, ENTIDAD ADAPTADA DE SALUD EAS que presta servicios de salud a los pensionados de los Ferrocarriles Nacionales de Colombia, Puertos de Colombia y a sus respectivos beneficiarios cuya misión es reconocer Prestaciones Económicas legales y Convencionales a los ex trabajadores, pensionados y beneficiarios de la liquidada empresa Ferrocarriles Nacionales de Colombia y ALCALIS. Así mismo, de administrar los servicios de salud a los pensionados y beneficiarios de la empresa liquidada Ferrocarriles Nacionales y Puertos de Colombia.

2.2 ANÁLISIS DE SU ENTORNO

Al hablar de análisis de entorno, se busca mencionar los aspectos que afectan directa e indirectamente el logro y cumplimiento de los objetivos institucionales, misión y visión y sus objetivos de seguridad de la información de la entidad Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia.

En vista de ello, el entorno está compuesto por cinco variables o factores, la Figura 1**: Análisis del entorno del Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia** ilustra el análisis del entorno del Fondo:

Figura 1. Análisis del entorno del Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia



Fuente de autores

En el Cuadro 1 **Matriz DOFA institucional Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia** se observa la matriz DOFA institucional del Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia.

Cuadro 1. Matriz DOFA institucional Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia

	Fortalezas	Debilidades
Matriz DOFA institucional Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia	-Estructura documental que soporta la gestión de la entidad. -Compromiso de la alta dirección y de los funcionarios de la entidad. -Sistemas de gestión de calidad fortalecida. -Plan de mejoramiento institucional. -Programa de auditorías internas. -Manuales. -Estructura basada en procesos. -Políticas y directrices para el funcionamiento de la entidad. -Controles preventivos y correctivos -Sistemas de información confiable. -Revisiones por la dirección semestrales.	-Falta de efectividad de las acciones implementadas en el plan de mejoramiento institucional. -Desactualización de la metodología para la administración del riesgo. -Baja participación de algunos funcionarios en la autoevaluación. -Falta de levantamiento de activos de información. -Falta de sistema integrado para el manejo de Peticiones, Quejas, Reclamos, Sugerencias y Denuncias -Falta de oportunidad en la respuesta de los trámites.
Oportunidades	**Estrategias (FO)**	**Estrategias (DO)**
Reorganización del estado que permita asumir nuevas funciones.	-Mejora continua de los sistemas de información. -Seguimiento permanente a los sistemas de comunicación, información y control. -Actualización permanente de las políticas y directrices acorde con el cambio normativo. -Revisión permanente de los procesos y procedimientos para que guarden el principio de interrelación.	-Fortalecer el plan de mejoramiento de manera efectiva. -Seguimiento permanente a los trámites de la entidad. -Diseñar políticas para mitigar el impacto de los riesgos de la entidad. -Sensibilización frente al fortalecimiento del autocontrol. -Establecer metodología para el levantamiento de los activos de información. -Revisión permanente de los procesos y procedimientos para que guarden el principio de interrelación.
Amenazas	**Estrategias (FA)**	**Estrategias (DA)**
Normatividad del sistema integral de salud. Liquidación de la Entidad.	-Mejora continua de los sistemas de información. -Revisión continúa del sistema de gestión.	Seguimiento permanente a los trámites generales. Sensibilización del sistema de gestión. Actualización constante de los riesgos de la entidad. Manejo adecuado de la comunicación. Diseñar políticas para la administración de la información. Implementar sistemas para el manejo de las PQRS.

Fuente: Formato ESDESOPSFO09 Matriz DOFA institucional FPS FN de Colombia. Bogotá, D.C, 2016

2.3 BENEFICIOS PARA LA EMPRESA DEL SGSI

Para el Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia, los beneficios que tendría al contar con un Sistema de Gestión de Seguridad de la

Información (SGSI), basado en el diseño del Modelo de Seguridad y Privacidad de la Información (MSPI) planteado en este documento, serían los siguientes:

- La entidad podrá garantizar la protección y privacidad de los datos de sus afiliados y usuarios respetando la legislación colombiana haciéndolo de una forma más controlada y eficaz.

- El Modelo de Seguridad y Privacidad de la Información (MSPI) permitirá a la entidad el preservar tanto la integridad, disponibilidad, confidencialidad y privacidad de su información mediante la correcta aplicación del Sistema de Gestión de Seguridad de la Información (SGSI).

- La entidad podrá sacar mayor provecho a las tecnologías de la información con las que cuenta, siendo más eficiente en sus procesos misionales.

- Permitirá que la entidad alcance un mejor estado en nivel de seguridad de la información, detectando riesgos, amenazas y vulnerabilidades y mejorando su respuesta frente a estas.

- El contar con un SGSI permitirá que la entidad tenga una panorámica completa y ordenada de todo su esquema de seguridad de la información, lo que indudablemente permitirá un mayor control del riesgo, un mejor aprovechamiento del tiempo, una focalización más rápida y controlada de incidentes y un flujo más rápido en cuanto a la realización de procesos repetitivos.

- La entidad podrá dar cumplimiento al eje de Seguridad y privacidad de la información de la estrategia de gobierno en línea (GEL) que busca guardar los datos de los ciudadanos como un tesoro, garantizando la seguridad de los mismos.

2.4 BENEFICIOS DE ADOPTAR EL ESTÁNDAR ISO 27001

Dentro de los beneficios que adoptar el estándar ISO 27001 trae para el Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia están:

- Permitir que la entidad pueda garantizar la continuidad del negocio mediante un plan de contingencia bien diseñado.

- Dar cumplimiento a la legislación y normativa colombiana vigente, tales como de Protección de datos personales y la estrategia de gobierno en línea (GEL).

- Reducir el impacto que tienen los riesgos de seguridad de la información dentro de la entidad al aumentar la seguridad de los sistemas de información de forma efectiva, planificada y mejor gestionada.

- Permitir la toma de conciencia del personal en relación a la importancia del correcto manejo y trato de la información, la aplicación adecuada de las medidas de seguridad y las responsabilidades tanto de los empleados como de la empresa en relación a la información con que interactúan y a los dueños de la misma.

- Permitir que la entidad pueda tener un ciclo de mejoramiento continuo mediante la metodología PHVA (Planificar, Hacer, Verificar y Actuar).

- Presentar a sus afiliados y usuarios, una mejor imagen en cuanto al tema de seguridad de la información, lo que conlleva a una mayor fidelización de los mismos al aumentar el nivel de confianza.

- Este estándar establece un tratamiento de la información en todos los procesos de la entidad, además de contar con un prestigio reconocido a nivel internacional.

- Otra ventaja de este estándar es la fácil interrelación que tiene con normas como la ISO 90001 (calidad), de igual manera con el resto de sistemas de gestión que existen en la entidad.

- Contar con mayor criterio a la hora de enfrentar riesgos, mediante procesos de acción enfocados y previamente planeados.

3. DISEÑO METODOLÓGICO

3.1 DIAGNÓSTICO DE SEGURIDAD DE LA EMPRESA

Este apartado presenta el diagnóstico que se realizó con el objetivo de identificar el estado actual que tiene la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

Como primer paso, se procedió a la identificación del nivel de estratificación de la entidad que permitió definir de antemano, el nivel de responsabilidad de la entidad en cuanto a la seguridad de la información. Para esto, se tomó como referencia el método planteado en el documento "Guía3: ESTRATIFICACIÓN DE ENTIDADES" del modelo de Modelo de Seguridad y Privacidad de la Información, anexo 3 del modelo seguridad de la información para la estrategia de Gobierno en Línea 2.0, el cual define tres tipos de estratos de entidades: bajo, medio y alto, y cuyo valor se obtiene al realizar una evaluación de los siguientes aspectos: Presupuesto de funcionamiento de la entidad, Infraestructura, los servicios ofrecidos en línea y el tamaño y capacidad del área de sistemas.[2]

A continuación se muestran las respuestas que fueron seleccionadas de acuerdo a la información suministrada por la entidad y el respectivo el puntaje asignado a cada una de ellas, puntajes que fueron sumados para así obtener el valor de estratificación de la entidad relacionada en la Cuadro 2 **Valoración estratificación de la entidad**.

Cuadro 2. Valoración Estratificación de la Entidad

	Presupuesto en Millones de Pesos	Existencia y Función del Área de Sistemas	No PC's	No Servidor	Existencia y Objeto de la WAN	Transaccionalidad en la WEB	Desarrollo de Software	No Empleados de Sistemas
Valor	4.676.022.580	Reactivas	261	9	Internet con servicios públicos ofrecidos	Transaccionalidad SI datos propios	No desarrolla software	4
Puntaje	3	2	2	2	2	2	1	1
Fuente: Autores								

[2] Anexo 3: Estratificación de Entidades - Modelo seguridad de la información para la estrategia de Gobierno en Línea 2.0, Pág. 8.

Se determina que el puntaje total de la estratificación establecido por la suma de los puntajes independientes obtenidos de cada una de las respuestas, para la entidad es igual 15 puntos. De acuerdo a los rangos de valores relacionados en la Cuadro 3 **Rangos de Estratificación de Entidades:**

Cuadro 3. Rangos de Estratificación de Entidades[3]

Puntos	Clasificación (Estrato)
Menor a 11	Bajo
Entre 11 y 22	Medio
	Alto
Fuente: Anexo 3: Estratificación de Entidades - Modelo seguridad de la información para la estrategia de Gobierno en Línea 2.0, Pág. 12	

El nivel de estratificación de la misma se encuentra clasificado en un nivel MEDIO, lo que inicialmente implicaría un esfuerzo considerable para los requerimientos del Modelo de Seguridad y Privacidad de la Información.

3.1.1 Resultados del análisis de brecha ISO 27001. Para la realización del análisis de brecha con los objetivos de control y controles definidos en el "Anexo A de la norma ISO/IEC 27001:2013, también se utilizó el "ANEXO A: Instrumento de evaluación MSPI 2016 FPS" referenciado en el presente documento, el cual contiene las preguntas que permiten identificar la línea base de seguridad administrativa y técnica, el nivel de madurez y las respectivas respuestas dadas por los usuarios de la entidad que además permite la definición una serie de acciones orientas a poder cerrar las brechas encontradas que deben ser implementadas por la entidad en las fases de planificación, de implementación, de evaluación de desempeño y de mejora continua del Modelo de Seguridad y Privacidad de la Información con el objetivo de asegurar la integridad, confidencialidad y disponibilidad de la información de la entidad.

Con base en la información recopilada, el Cuadro 4 muestra los resultados del análisis, donde se observa que la calificación actual de la entidad con relación a los controles del Anexo de la norma ISO 27001:2013, es de 23%.

[3]Anexo 3: Estratificación de Entidades - Modelo seguridad de la información para la estrategia de Gobierno en Línea 2.0, Pág. 12.

Cuadro 4. Calificación actual controles Anexo A ISO 27001:2013

Número	Evaluación de Efectividad de controles			
	Dominio	Calificación Actual	Calificación Objetivo	Evaluación de efectividad de control
A.5	Políticas de seguridad de la información	30	60	**Repetible**
A.6	Organización de la seguridad de la información	26	60	**Repetible**
A.7	Seguridad de los recursos humanos	31	60	**Repetible**
A.8	Gestión de activos	24	60	**Repetible**
A.9	Control de acceso	9	60	**Inicial**
A.10	Criptografía	0	60	**Inexistente**
A.11	Seguridad física y del entorno	0	60	**Inexistente**
A.12	Seguridad de las operaciones	6	60	**Inicial**
A.13	Seguridad de las comunicaciones	0	60	**Inexistente**
A.14	Adquisición, desarrollo y mantenimiento de sistemas	1	60	**Inexistente**
A.15	Relaciones con los proveedores	10	60	**Inicial**
A.16	Gestión de incidentes de seguridad de la información	20	60	**Inicial**
A.17	Aspectos de seguridad de la información de la gestión de la continuidad del negocio	10	60	**Inicial**
A.18	Cumplimiento	27,5	60	**Repetible**
PROMEDIO EVALUACIÓN DE CONTROLES		**14**	**60**	**Inicial**

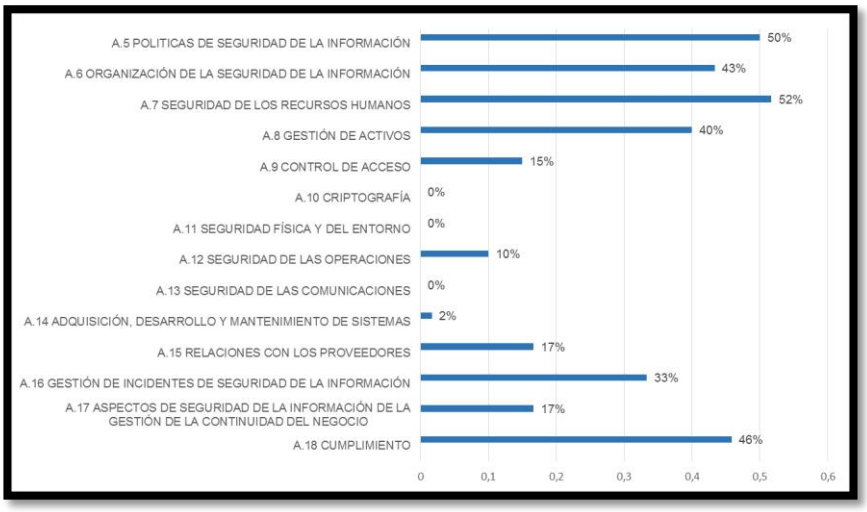
Fuente: Instrumento de evaluación MSPI del MINTIC

Lo anterior significa que el Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia se encuentra en un nivel de madurez Inicial de acuerdo a la valoración de los controles del Anexo A ISO 27001:2013, que corresponde que la entidad ha reconocido que tiene un problema en cuanto a la gestión de seguridad de la información y que debe tratarlo, teniendo en cuenta que no posee procesos estandarizados, que los controles implementados por cada uno de los miembros de la misma se hacen de manera reactiva y que a pesar de que tiene algunos de estos procedimientos documentados, estos no se han dado a conocer de manera adecuada y/o no se aplican.

Por lo tanto le implicará a la entidad un gran esfuerzo debido a la baja calificación en la efectividad y ausencia de controles de muchos de ellos; por ello para garantizar su efectividad la entidad requerirá la adquisición, adecuación o mejora de mecanismos y herramientas tecnológicas, lo que implica, que la entidad deberá adelantar procesos de contratación para la adquisición de soluciones tecnológicas cuyos costos pueden ser elevados y su implementación puede demandar un tiempo considerable.

El resultado de la evaluación de cada uno de los objetivos de control del Anexo A de la norma ISO/IEC 27001:2013 se ilustra en la Figura 2.

Figura 2. Nivel Cumplimiento Objetivos de Control Anexo A ISO 27001:2013



Fuente: Autores

De acuerdo a los resultados de la evaluación de la efectividad de los controles del Anexo A ISO 27001:2013, el nivel de cumplimiento es del 60%, se observa en la Figura 2 que algunos controles tiene un porcentaje de cumplimiento bajo, como los que lista la Tabla 1.

Tabla 1. Objetivos de control con nivel BAJO de cumplimiento

Objetivos de control con nivel bajo de cumplimiento	**Porcentaje**
A.10 Criptografía	0%
A.11 Seguridad física y del entorno	0%
A.13 Seguridad de las comunicaciones	0%
A.14 Adquisición, desarrollo y mantenimiento de sistemas	2%
A.9 Control de acceso	15%
A.15 Relaciones con los proveedores	17%
A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio	17%
Fuente: Autores	

Lo cual indica que la entidad debe buscar e implementar mecanismos, procedimientos y herramientas tecnológicas para limitar el acceso a información y

a instalaciones de procesamiento de información, asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios, hacer que los usuarios rindan cuentas por la salvaguarda de la información de autenticación, asegurar el uso de criptografía, prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización, prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización, asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte, mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa, garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida, asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información, asegurar la protección de los datos usados para pruebas, asegurar la protección de los activos de la organización que sean accesibles a los proveedores, mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores y Asegurar la disponibilidad de instalaciones de procesamiento de información.

3.1.2 Resultados del análisis del contexto de seguridad. Con base al análisis del estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad y la identificación de algunas situaciones que de alguna otra manera afectan su seguridad, el Cuadro 5 ilustra los resultados del análisis del contexto de seguridad.

Cuadro 5. Análisis del contexto de seguridad

	Fortalezas	**Debilidades**
Análisis interno	Apoyo de alta dirección para la implementación del sistema de gestión de seguridad de la información. Política de seguridad debidamente aprobada y socializada al interior de la Entidad, por la alta Dirección.	Falta de gestión de riesgo de seguridad de la información. Falta de controles para asegurar una adecuada protección de su confidencialidad e integridad de la información. Falta de planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos las operaciones esenciales, manteniendo las consideraciones en seguridad de la información utilizada en los planes de continuidad y función de los resultados del análisis de riesgos. Falta de concienciación, aprobación y conocimiento en temas seguridad y privacidad por parte de los funcionarios.
	Oportunidades	**Amenazas**
Análisis externo	Implementación de nuevas tecnologías para aumentar la eficiencia y asegurar la gestión del riesgo de seguridad de la información. Apropiación de un modelo de seguridad y privacidad de la información acorde a la legislación colombiana que garantice la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad.	Falta de recurso para renovar la infraestructura tecnología Política de austeridad Obsolescencia de equipos
Fuente de actores, basada en datos del Instrumento de evaluación MSPI del MINTIC		

De igual manera, se encontró que la entidad cuenta con un nivel inicial, debido a que se no cuenta con una identificación de activos ni gestión de riesgos relacionados puntualmente con la seguridad de la información, lo que no permite determinar la criticidad de la información que se maneja y por tanto los controles que se tienen en el momento de realizar el diagnostico, no están alineados con el objeto de preservar la integridad, disponibilidad y confidencialidad de la información.

Por otra parte, teniendo en cuenta que la herramienta de diagnóstico del MINTIC que se utilizó, cuenta con un componente de ciberdefensa, se aclara que esta parte está fuera del alcance de este proyecto.

3.1.3 Resultados de análisis de necesidades de seguridad. Esta sección se centra en la presentación de los datos relacionados con los requisitos, necesidades y/o expectativas de las partes interesadas de la entidad con respecto a la seguridad de la información que de una u otra manera afectan la capacidad para lograr los resultados previstos por el sistema de gestión de seguridad de la información.

Las partes interesadas de la entidad se clasifican en cliente interno y cliente externos que para el Fondo son los siguientes:

Cliente Interno:

Funcionarios, Contratista, Empleados de Servicios de Generales.

Cliente Externo:

- Ex trabajadores, pensionados y beneficiarios de Ferrocarriles Nacionales de Colombia.

- Ex trabajadores, pensionados y beneficiarios de Prosocial.

- Pensionados y beneficiarios de la Fundación San Juan de Dios e Instituto Materno Infantil.

- Ex trabajadores, pensionados y beneficiarios de álcalis de Colombia.

- Colpensiones - Administradoras de Pensiones.

- Unidad de Gestión Pensional y Parafiscales, UGPP.

- Fondo de Pensiones Públicas de Nivel Nacional de Colombia, FOPEP.

- Entes de control.

- Proveedores.

- Contratista de salud.

El resultado del análisis de las partes interesadas se ilustra en el Cuadro 6, donde es notable que sus intereses son la garantía de la protección de los datos personales y la reserva de la información considerada como sensible.

Cuadro 6. Necesidades y expectativas de las partes interesadas

Partes Interesada		Necesidades y expectativas
Cliente interno	Funcionarios Contratista Empleados de Servicios de Generales	Cumplimiento de las obligaciones legales Garantía de privacidad de sus datos personales Restricciones de acceso y de tratamiento de información de la entidad con terceros. Mantener un sistema de información en línea confiable y disponible para todos los usuarios del FPS y ciudadanos, que permita una retroalimentación constante
	Ex trabajadores, pensionados y beneficiarios de Ferrocarriles Nacionales de Colombia Ex trabajadores, pensionados y beneficiarios de Prosocial Pensionados y beneficiarios de la Fundación San Juan de Dios e Instituto Materno Infantil Ex trabajadores, pensionados y beneficiarios de álcalis de Colombia	Protección de Datos Personales Herramientas que garanticen la seguridad de sus registros evitando la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Calidad en los servicios prestados a través de la tecnología de información y comunicación. Cumplimiento de obligaciones legales vigentes
	Colpensiones - Administradoras de Pensiones Unidad de Gestión Pensional y Parafiscales, UGPP Fondo de Pensiones Públicas de Nivel Nacional de Colombia, FOPEP	Garantía de la integridad y confidencialidad de la información suministrada para ejercicio de sus funciones. Garantía a la reserva de la información

Cuadro 6. (Continuación)

	Partes Interesada	Necesidades y expectativas
Cliente Externo	Entes de Control	Garantía de Integridad de los datos protegidos Aportar la identificación de las infraestructuras críticas para la mejora de respuesta ante las amenazas que afectan la Seguridad Digital Compromiso para la construcción de un Estado más eficiente, más transparente y participativo.
	Proveedores	Gestión de Acuerdos de niveles de servicios de manera adecuada. Gestión de cambios en los servicios prestados.
	Contratista de Salud	Garantía de la disponibilidad de los sistemas de información para ejercicios de sus funciones
Fuente: Autores		

3.2 DISEÑO DEL SGSI

3.2.1 Alcance del SGSI. El alcance permite determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información de la entidad[4].

El alcance del 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 modelo 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.

[4]Norma ISO/IEC 27001:2013, Pág. 2

Este proyecto, cubre el diseño del modelo de seguridad y privacidad de la información, basada en los requerimientos de la estrategia de gobierno en línea, el cual implica la primera fase de la implementación de un Sistema de Gestión de Seguridad de la Información, que corresponde a la etapa de planeación.

Para el desarrollo de este proyecto, se usará como guía, la norma ISO 27001-2013, que especifica los requisitos necesarios para todas las fases por las que pasa un Sistema de Gestión de Seguridad de la Información.

3.2.2 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, la seguridad de la información busca la disminución en el impacto generado sobre sus activos, 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.

De acuerdo con lo anterior, esta política aplica a la entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinados por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.

- Cumplir con los principios de seguridad de la información.

- Cumplir con los principios de la función administrativa.

- Mantener la confianza de sus usuarios y funcionarios.

- Apoyar la innovación tecnológica.

- Proteger los activos tecnológicos.

- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros y usuarios del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA.

- Garantizar la continuidad de la entidad frente a incidentes.

- El FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA ha decidido implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Esta política aplica a toda la entidad, sus funcionarios, terceros, proveedores del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA y la ciudadanía en general.

A continuación se establecen las 21 Reglas de seguridad que soportan el SGSI del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA:

- Definirá, Implementará, Operará y Mejorará de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de la entidad, y a los requerimientos regulatorios.

- Definirá las responsabilidades frente a la seguridad de la información compartida, publicada y aceptada por cada uno de los funcionarios, proveedores o terceros.

- Protegerá la información generada, procesada o resguardada por los procesos, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

- Definirá y Establecerá controles de acuerdo con la clasificación de la información de su propiedad o en custodia para proteger la información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto, accesos no autorizados, violaciones y perdida de integridad de la información.

- Protegerá su información de las amenazas originadas por parte del personal.

- Protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- Controlará la operación de sus procesos garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- Implementará control de acceso a la información, sistemas y recursos de red.

- Garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

Garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- Garantizará la disponibilidad de sus procesos y la continuidad de su operación basada en el impacto que pueden generar los eventos.

- Garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

- Solo permitirá el uso de software autorizado y/o adquirido legalmente por la entidad.

- Todos los funcionarios y/o contratistas, serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

Todos los funcionarios y/o contratistas, serán responsables de reportar los incidentes de seguridad, mal uso de los recursos y eventos sospechosos de los que tenga conocimiento.

- Todos los funcionarios y/o contratistas, deberán acatar y dar cumplimiento a los lineamientos dispuestos en el manual de uso del Sistema de Gestión de Seguridad de la Información.

- Todos los equipos de propiedad del Fondo deben contar con la fecha y hora exactas para que el registro de los archivos de auditoría sea el correcto.

- Cualquier auditoría de seguridad a los sistemas del fondo debe estar debidamente autorizada y aprobada por el jefe de oficina asesora de Planeación y sistemas, con visto bueno del Director.

- Las auditorías de seguridad de la información deben ser realizadas por personal preparado técnicamente, en caso de no existir, el personal asignado debe ser capacitado adecuadamente.

- Las claves y contraseñas asignadas a cada funcionario son de carácter personal e intransferible, su uso debe ser de manera responsable, tener un buen manejo, efectuar cambios de manera periódica y por seguridad deben ser alfanumérica de mínimo 8 caracteres e incluir Mayúsculas y minúsculas; No se permite el préstamo de claves y contraseñas.

- Cumplir con la política de buen uso y manejo de los equipos de cómputo, los servicios institucionales de correo electrónico e internet. Esta política de seguridad

deberá seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, desarrollo de nuevos servicios, nuevos lineamientos normativos o de ley, entre otros.

Para mayor detalle de la política general de seguridad de la información del Fondo, ver el “ANEXO B: Política General y Específicas Seguridad de la Información FPS” referenciado en el presente documento.

3.2.3 Roles y responsabilidades de seguridad. Los siguientes son los roles y responsabilidad del Sistema de Gestión de Seguridad de la Información que se definieron, los cuales están incluidos en la política general de seguridad y privacidad de la información del presente trabajo de grado.

La distribución de roles y responsabilidades estará representada en la Figura 3, en la cual se presentan los perfiles de manera genérica el nivel al cual pertenecerían según lo propuesto.

Figura 3. Equipo de Gestión de Seguridad de la Información

Fuentes: autores

Comité de gobierno en línea y anti trámites y cero papel (comité de desarrollo administrativo)

- Revisar los diagnósticos del estado de la seguridad de la información de la entidad.

- Acompañar e impulsar el desarrollo de proyectos de seguridad.

- Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de Nombre de la entidad.

- Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.

- Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.

- Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.

- Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.

- Informar a la Dirección de la entidad acerca del desempeño del SGSI y de la manera como se están gestionando los planes asociados a la seguridad y privacidad de la información.

- Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.

- Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma.

- Garantizar el logro de la política y objetivos de Seguridad de la Información.

- Aprobar y hacer seguimiento a los niveles de aceptación riesgos de seguridad de la información y documentación requerida por la norma seleccionada.

- Analizar los datos arrojados por el SGSI y tomar las decisiones necesarias para garantizar el mantenimiento y mejoramiento del sistema.

- Garantizar los recursos para contribuir, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI.

- Las demás funciones inherentes a la naturaleza del Comité.

Responsable y/o encargado de seguridad de la información

- Orientar a la entidad al cumplimiento de los requisitos de Seguridad de la Información exigidos por la estrategia de gobierno en línea y la legislación vigente.

- Planificar y ejecutar las actividades de Seguridad de la Información que involucren a todo el personal de la entidad.

- Efectuar seguimiento y control del SGSI, aplicando los controles, correctivos y ajustes necesarios para el logro de los objetivos, informando a la alta dirección sobre el desempeño del sistema.

- Cumplir con las medidas de Seguridad en la Información que se definan en los procedimientos de trabajo que se elaboren para las diferentes actividades que se desarrollen en la entidad.

- Establecer, comunicar y revisar los objetivos y la política de seguridad de la información.

- Cumplir con el plan de comunicación, sensibilización y comunicación definido en el SGSI.

- Respetar y cumplir los principios básicos de seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

- Implementar las mejoras identificadas en el SGSI.

- Desarrollar las políticas de seguridad de la información al interior de la entidad, liderar, coordinar su implementación con la participación activa de las dependencias de la Entidad y velar por su correcta aplicación.

- Revisar la efectividad de los controles establecidos y coordinar la implementación de controles específicos para nuevos sistemas de información o servicios informáticos.

- Impulsar la cultura de seguridad de la información dentro de la entidad.

- Reportar y atender a los requerimientos de seguridad antes los equipos de respuestas a incidentes (CSIRT PONAL, Ministerios, entre otros) que lo requieran.

- Constituir un programa periódico (por lo menos una vez al año) para la revisión de vulnerabilidades de la plataforma tecnológica de la Entidad y coordinar los respectivos aseguramientos o acciones conforme los resultados de las mencionadas pruebas.

- Mantener un inventario de los activos de información en la entidad y clasificarlos según sea su tipo con la con la participación activa de las dependencias de la Entidad.

- Monitorear el avance general de la gestión y tratamiento de riesgos que permita el control de las amenazas.

- Identificar las necesidades y recursos necesarios (tecnológicos, humanos, de capacitación, financieros, etc.) Para el mantenimiento de la infraestructura de seguridad de la información.

- Realizar seguimiento al SGSI.

- Actuar como un asesor en seguridad de la información para la Entidad.

- Hacer seguimiento al comportamiento de los indicadores de gestión de la seguridad de la información que adopte el Comité de desarrollo administrativo.

- Hacer la evaluación del desempeño del SGSI.

- Presentar y reportar al Comité de desarrollo administrativo el estado y monitoreo de los incidentes de seguridad de la información, los resultados de las auditorias periódicas y la revisión del SGSI.

- Establecer puntos de enlaces con encargados de seguridad de la información de otras entidades y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.

- Revisar periódicamente los niveles de acceso a los sistemas de información.

- Determinar los requerimientos de copias de respaldo para la información de la entidad.

- Tomar las acciones adecuadas en caso de violaciones de seguridad.

- Verificar periódicamente la integridad y coherencia de la información producto de los procesos.

- Las demás que le asigne el director general.

Responsable y/o encargado de protección de datos

- Impulsar una cultura de protección de datos dentro de la entidad.

- Mantener un inventario de las bases de datos personales en poder de la entidad y clasificarlas según su tipo.

- Registrar las bases de datos de la entidad en el registro Nacional de bases de datos y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita al SIC.

- Integrar las políticas de protección de datos dentro de las actividades de las demás procesos de la entidad (talento Humano, Gestión TIC´S, proveedores).

- Coordinar la definición e implementación de los controles para la gestión de riesgo del tratamiento de datos personales.

- Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales.

- Tramitar las consultas, solicitudes y reclamos.

- Utilizar únicamente los datos personales que hayan sido obtenidos mediante autorización, a menos que los mismos no la requieran.

- Respetar las condiciones de seguridad y privacidad de información del titular.

- Cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente.

- Realizar un entrenamiento general en protección de datos para todos los empleados de la entidad.

Responsable de los procesos

Propietario de la información: son los jefes o encargados 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.

Entre las responsabilidades de los propietarios de información se tienen:

- Clasificar la información a su cargo y asegurar que los controles apropiados están definidos y funcionan en orden a garantizar la integridad, confidencialidad y disponibilidad de los sistemas de TI y de sus datos.

- Asignar los niveles iníciales de clasificación de información.

- Revisión y actualización periódica (por lo menos una vez al año) de la clasificación de la información con el propósito de verificar que cumpla con los requerimientos de la entidad y leyes vigentes.

- Determinar los criterios y niveles de acceso a la información.

- Definir los controles de seguridad para la información que tiene a su cargo

Custodio de la información: En el fondo los encargados de la custodia de la información son los procesos de Gestión Documental y Gestión de Tic´s quienes tiene la responsabilidad de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido.

Entre las principales responsabilidades de los custodios de la información se tienen:

Aplicar las políticas, procedimientos y protocolos asociados al acceso a la información que se establezcan por parte de la entidad y del propietario de la información (propietario de los activos), así como los relacionados con su trámite y conservación.

Usuarios de la información: Son todos los funcionarios, contratistas, proveedores, entidades que con la debida autorización del propietario de la información, pueden generar 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.

Los usuarios solo deben tener acceso a la información a la que están autorizados a consultar y procesar. Las autorizaciones que se otorguen limitaran su capacidad en los entornos informáticos de forma que no puedan realizar actividades diferentes a las autorizadas.

Las responsabilidades de los usuarios finales, es decir, aquellas personas que utilizan información del Fondo como parte de su trabajo diario están definidas a continuación:

Funcionarios

- Reportar e identificar actos condiciones inseguras durante el desarrollo de las actividades.

- Respetar y cumplir los principios básicos de seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

- Dar cumplimiento a las políticas y procedimientos establecidos en el SGSI.

- Mantener la confidencialidad de las contraseñas de aplicaciones y sistemas.

- Cumplir con los controles establecimientos en las políticas y procedimientos de seguridad de la información definidos por la entidad.

- Comunicar los incidentes relativos de la seguridad de información.

- Asegurarse de ingresar información adecuada a los sistemas.

- Utilizar la información únicamente para los propósitos autorizados.

- Tomar las medidas adecuadas para evitar que la información se divulgue o use sin autorización.

Ciudadanos

- Cumplir con todas las medidas de seguridad definidas en la política de Seguridad de la Información.

- Participar activamente de las capacitaciones periódicas de la política de Seguridad de la Información.

Proveedores

Dar cumplimiento a las actividades descritas en los acuerdos de Nivel de servicios del SGSI.

- Dar cumplimiento a las políticas y procedimientos establecidos en el SGSI

• Velar por la protección de los activos de la entidad frente a distintas amenazas, durante el tiempo y forma que se establezca en la relación contractual, en base a los requerimientos legales, reglamentarios y empresariales.

• Garantizar el cumplimiento de los requerimientos establecidos por la Ley estatutaria de Protección de Datos Personales y las medidas identificadas en el Decreto que la reglamenta. Del mismo modo, el proveedor asignado como encargado de tratamiento de ficheros de la entidad con datos de carácter personal cumplirá los requerimientos establecidos por la entidad como propietario de dichos ficheros.

3.2.4 Procedimiento de riesgos. El procedimiento de riesgo que manejará la entidad tomará como base el "ANEXO C: Guía metodológica de análisis de riesgos de seguridad y privacidad de la información FPS" que se encuentra referenciado en este documento y donde se detalla todo, sin embargo, se dará un contexto a continuación:

Para la metodología de evaluación y tratamiento de riesgo es importante realizar un análisis inicial relacionado con el estado actual de la estructura de riesgo y gestión en la entidad, desde un punto de vista estratégico; para ello se estructura la metodología resumida en la Tabla 2.

Tabla 2. Etapas de la gestión del riesgo a lo largo del MSPI

Etapas del MSPI	
Planear	Establecer Contexto, valoración del riesgo, planificación del tratamiento del riesgo, aceptación del riesgo
Implementar	Implementación del plan de tratamiento de riesgo
Gestionar	Monitoreo y revisión continua de los riesgos
Mejora continua	Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información
Fuente: Autores	

3.2.4.1 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.

3.2.4.2 Valoración del riesgo. Esta actividad se realiza con base en las causas internas o externas identificadas por los procesos a través del contexto estratégico, describiendo cuales son los activos críticos asociados a los procesos y cuales contienen información sensible. Para ello es necesario definir los siguientes términos que permiten entender esta actividad, y se listan a continuación:

- Proceso
- Objetivo del proceso
- Identificación de activos
- Riesgo
- Causas (amenazas y vulnerabilidades)
- Descripción del riesgo
- Efectos de la materialización del Riesgo

3.2.4.3 Planificación del tratamiento del riego. En este paso se toman los resultados de la etapa anterior donde se ha establecido la zona de riesgo determinada por el desplazamiento dentro de la Matriz de Evaluación y Calificación y la nueva valoración de acuerdo a los controles identificados y esta manera se determinará finalmente la selección de las opciones de tratamiento del riesgo, así:

- Evitar el riesgo decidiendo no iniciar o continuar la actividad que lo originó.
- Tomar o incrementar el riesgo con el fin de perseguir una oportunidad.
- Retirar la fuente del riesgo.
- Cambiar la probabilidad.

- Cambiar las consecuencias.

- Compartir el riesgo con una o varias de las partes (incluyendo los contratos y la financiación del riesgo).

- Retener el riesgo a través de la decisión informada.

Lo anterior teniendo en cuenta equilibro del costo y el esfuerzos de la implementación frente a los beneficios derivados con respecto a los requisitos legales, reglamentarios y otros, como la responsabilidad social y la protección del medio ambiente.

3.2.4.4 Aceptación del riego

- Durante la etapa de evaluación de riesgos se aceptan aquellos riesgos de zona de riesgo “baja” y “moderada”, y no se aceptan los riesgos de zona l “Alto” y “externa” los cuales deben ser tratados o transferirlos .

- Durante la etapa de tratamiento de riesgos se aceptará el riesgo siempre y cuando el costo beneficio sea negativo y no afecte la política de seguridad.

Por ello la entidad teniendo en cuenta los criterios descritos a continuación, se establecen las tablas del “Anexo C: Guía metodológica de análisis de riesgos de seguridad y privacidad de la información FPS”, donde determinada de manera cuantitativa y cualitativa los criterios de evaluación del riesgo, criterios de impacto, criterio de aceptación del riesgo.

Así, se pueden seguir definiendo otros criterios de aceptación de riesgos los cuales se emplearán durante el tratamiento, teniendo en cuenta el mapa de calor de la Cuadro 7.

Cuadro 7. Mapa de Calor

Casi seguro	*5*	A	A	E	E	E
Probable	*4*	M	A	A	E	E
Posible	*3*	B	M	A	E	E
Improbable	*2*	B	B	M	A	E
Raro	*1*	B	B	M	A	A
Probabilidad		*1*	*2*	*3*	*4*	*5*
		Insignificante	*Menor*	*Moderado*	*Mayor*	*Catastrófico*
		Impacto				

Fuente: Autores

Para mayor detalle de la metodología en todos sus aspectos, remitirse al anexo antes mencionado.

3.2.5 Objetivos de seguridad

3.2.5.1 Objetivo general. Diseñar un plan de seguridad y privacidad de la información mediante la aplicación de la estrategia de gobierno en línea y la norma ISO 27001:2013 con el fin de implementar un sistema de gestión de seguridad de la información dentro del Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia durante la vigencia 2017.

3.2.5.2 Objetivos específicos

- 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.

- Establecer una política de seguridad y privacidad de la información donde se evidencie el compromiso de la alta dirección frente al aseguramiento la seguridad asociada al recurso humano, físico y ambiental y a la administración del riesgo de seguridad de la información.

- Realizar capacitación, sensibilización y comunicación de la seguridad y privacidad de la información, asegurando que cada uno cumpla con sus roles y responsabilidades de seguridad y privacidad de la información dentro de la entidad.

- Revisar periódicamente el cumplimiento de los requisitos legales que en materia de seguridad y privacidad de la información apliquen a la entidad

3.2.6 Indicadores de la seguridad. Para el Fondo de Pasivo Social Ferrocarriles Nacionales de Colombia, se establecieron dos indicadores de gestión que servirán como insumo para la mejora continua del modelo de seguridad y privacidad de la información.

Los indiciadores establecidos fueron:

- Ataques informáticos a la entidad, cuyo objetivo es conocer el número de ataques informáticos que recibe la entidad.

- Incidentes de seguridad de la información, cuyo objetivo es garantizar la administración de incidentes de seguridad en la entidad.

- Revisiones de la seguridad de la información, cuyo objetivo es garantizar que se implementa y opera la seguridad de la información de acuerdo a las políticas y procedimientos de la entidad.

- Sensibilización y toma de conciencia, cuyo objetivo es establecer la efectividad de un plan de capacitación y sensibilización previamente definido como medio de prevención de incidentes de seguridad.

Dentro del objeto de estos indicadores, también se encuentran:

- Evaluar la efectividad de los controles de seguridad que se implementen.

- Evaluar la eficiencia del modelo de seguridad y privacidad de la información.

- Mejora continua del modelo.

- Servir como insumos al plan de gestión de riesgos.

- Comunicar valores de seguridad al interior de la entidad.

Para mayor detalle de los indicadores, ver “ANEXO D: Hoja de Vida Indicadores FPS” referenciado en este documento.

3.3 ANÁLISIS DE RIESGOS DE SEGURIDAD

3.3.1 Lista de activos de información. Para listar los activos de información de la entidad que fueron identificados, se utilizó el “ANEXO E: Inventario Activos Datos-Información FPS” referenciado en este documento y donde se presenta el detalle de cada activo, donde se incluye el nombre, la descripción, el área responsable, medio de conservación, ubicación y acceso, clasificación de la información (publica, clasificada o de uso interno), valoración del activo en cuanto a confidencialidad, integridad y disponibilidad, criticidad, fundamentos de ley, entre otros.

En este listado, se identificaron 4 tipos de activos:

- Servicios: Que contempla los servicios prestados por el sistema.

- Recurso Humano: Personas relacionadas con los diferentes sistemas.

- Activo de Información: Ficheros, copias de respaldo, datos de gestión interna, credenciales, datos de validación de credenciales, datos de control de acceso, registro de actividad entre otros.

- Activo de Software: Programas, aplicativos, desarrollos, software base, sistema de información.

En total se identificaron 118 activos que fueron tomados en cuenta para el análisis de riesgos. En el cuadro 8 se puede ver el esquema del formato que se diligenció.

Cuadro 8. Formato tabla de activos de Información

Información del Activo			Ubicación y acceso		Propiedad	Clasificación de la Información		Valoración del Activo de Información			
Tipo de Activo	Nombre del Activo	Desc.	Medio	Formato	Proceso Custodio	Ley 1712	Ley 1581	C	I	D	Criticidad
Fuente: Autores											

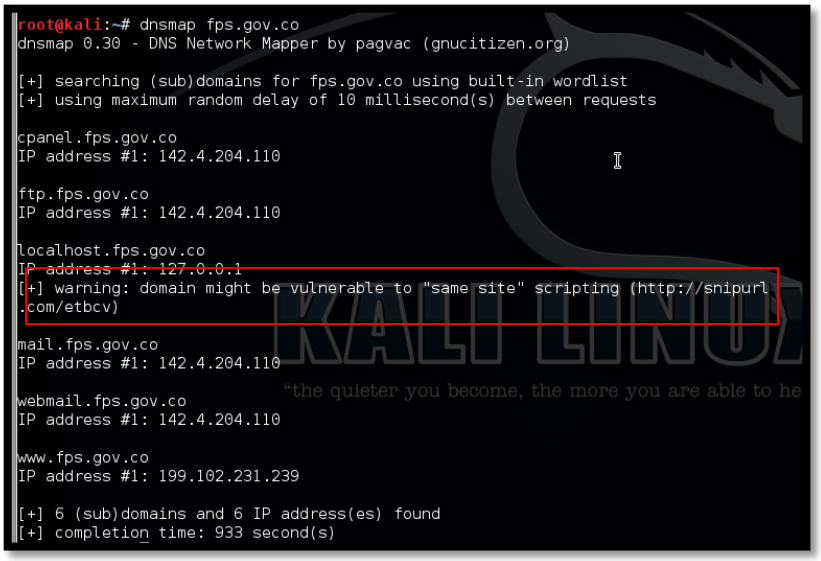
3.3.2 Lista de amenazas y vulnerabilidades. Con el fin de identificar y listar las amenazas y vulnerabilidades más relevantes con que cuenta la entidad Fondo de Pasivo Social de Ferrocarriles de Colombia, se procedió a utilizar la técnica de evaluación de la NIST SP800-115 basada en la metodología abierta de testeo de seguridad y que permite identificar sistemas, puertos, servicios y vulnerabilidades potenciales mediante el uso de herramientas tecnológicas o de forma manual.

Con previa aprobación del personal del proceso de Gestión TIC´S para así evitar cualquier ilegalidad o conflicto, se realizaron las siguientes actividades contenidas en el “ANEXO H: Reconocimiento Vulnerabilidades Fondo Pasivo Social” referenciado en el presente documento y donde sobresale lo siguiente:

Subdominio/IP

Lo primero que se hizo, fue una búsqueda de posibles IP de equipos del dominio de la entidad, esto desde una máquina virtual kali, utilizando DSNMAP, encontrando un total de 6 direcciones IP como se observa en la Figura 4.

Figura 4. Búsqueda de direcciones ip



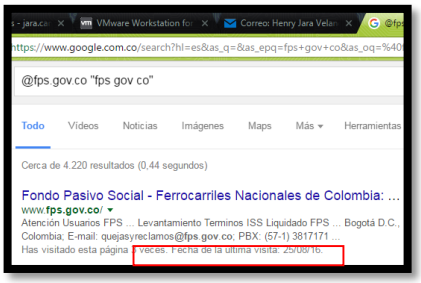
Fuentes: autores

Teniendo en cuenta lo anterior, se identificó que el dominio podría ser vulnerable a secuencias de comandos o Crosssite scripting.

Cuentas de correo

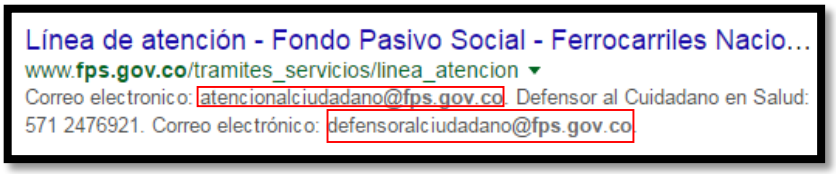
Después, se realizó una búsqueda de correos electrónicos de empleados de la entidad, mediante la búsqueda avanzada de Google, con el fin de identificar la estructura para la creación de correos y ver qué tan cuidadosos son al dejar información como esta en la red, los resultados se observan en las Figuras 4 a 8.

Figura 4. Correos encontrados



Fuentes: autores

Figura 5. Correos encontrados

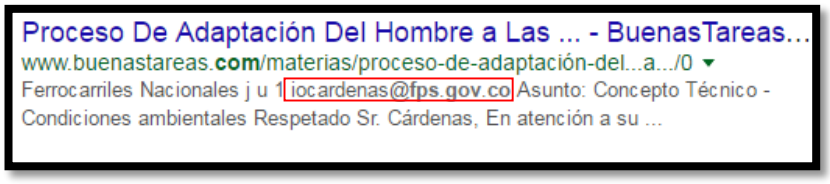


Fuentes: autores

Figura 6. Correos encontrados

Fuentes: autores

Figura 7. Correos encontrados



Fuentes: autores

Se obtuvieron direcciones de interés público como quejasyreclamos@fps.gov.co, atencionalciudadano@fps.gov.co y defensoralciudadano@fps.gov.co, pero adicional a ello, se obtuvieron algunos contactos como: nancybautista@fps.gov.co, Hernando.penaloza@fps.gov.co y iocardenas@fps.gov.co, correos que claramente son de empleados de la entidad y que al estar volando por la red, pueden ser recolectado por bots y hacer que los dueños de este, reciban correos fraudulentos o con software malicioso.

Información de Sitio Web

Por medio de la página web Whois, se realizó una búsqueda de información del sitio web, sin embargo se encontró que este dominio se reporta como disponible como se ve en la Figura 8.

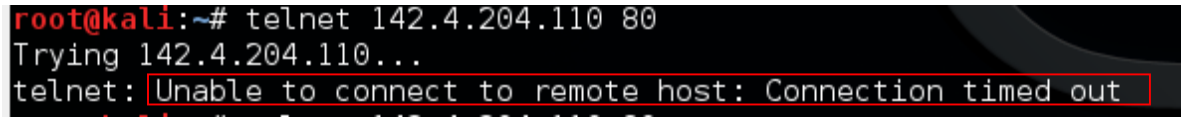
Figura 8. Página Whois

Fuentes: autores

Sistema Operativo

Del mismo modo se trató de hacer un reconocimiento al sistema operativo donde está la página web pero no se logró debido a la seguridad que tiene la entidad al respecto, esto se ve en la Figura 9.

Figura 9. Reconocimiento SO



Fuente: autores

Escaneo de Vulnerabilidades

Otra de las herramientas utilizadas fue OWASP ZAP, cuyo reporte se encuentra en el “ANEXO I: ZAP vulnerabilidades FPS” referenciado al final de este documento y donde se identificaron tres vulnerabilidades del sitio web descritas en la Tabla 3.

Tabla 3. Resultado ZAP

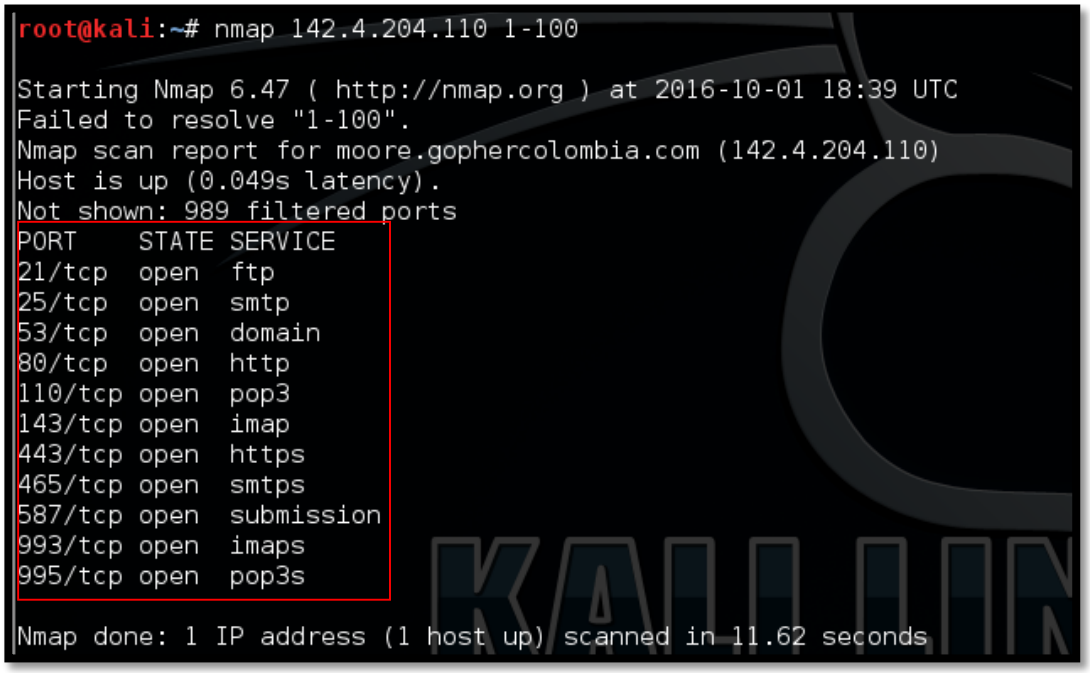
Criticidad	Vulnerabilidad
Low (Medium)	Cross-Domain JavaScript Source File Inclusion
Low (Medium)	**Web Browser XSS Protection Not Enabled**
Low (Medium)	**X-Content-Type-Options Header Missing**

Fuente: Reporte ZAP

Identificación de puerto y servicios

Adicionalmente, se realizó un escaneo de puertos del 1 al 100, encontrando abiertos los puertos Que se ven en la Figura 10.

Figura 10. Escaneo Puertos



Fuente: autores

Después de realizado este análisis, se encontraron vulnerabilidades como:

• La información como cuentas de correo electrónico de empleados de la entidad, que puede ser usada para él envió de correos fraudulentos, software malicioso o ingeniería social.

• El Crossdomain java script source file inclusion: Esta vulnerabilidad está presente porque no se asegura que la entrada de datos de terceros, este codificada de manera adecuada o porque no se verifica que los datos sean seguros en el momento que ingresan y se incluyen en la página de salida, en el caso de la entidad, los datos considerados como no confiables están basados en el contexto HTML, más puntualmente en Java script.

• web browser XSS Protection no tenabled: es un error en la configuración ya que no está habilitada la protección contra el Cross Site Scripting.

• X content type options header missing: es un error ya que al no tener habilitada esta cabecera cabe la posibilidad de que se carguen hojas de estilo o scripts maliciosos.

Puertos abiertos vulnerables como:

• 21FTP: tiene muchas vulnerabilidades de seguridad conocidas, un servidor ftp mal configurado puede permitir transferencia de ficheros, troyanos entre otros.

• 25 SMTP: tiene una larga trayectoria de vulnerabilidades, cualquier atacante examinaría detenidamente este puerto.

• 80 HTTP: cada día se descubren nuevos fallos de seguridad en los servidores web, pero al ser usado por la entidad, se recomienda tener mayor atención.

• 110 POP3: puede suponer un riesgo si se usa un servidor pop3 inseguro.

• 143 IMAP: es probablemente uno de los puertos más escaneados, es un sistema relativamente nuevo y dado que sus servidores no han tenido tiempo de maduración, este puerto es susceptible a muchos ataques.

• 443 HTTPS: este puerto no debería estar abierto a menos que realmente se use para comercio seguro vía web.

Una vez realizados los procedimientos anteriores, se elaboró un listado completo de vulnerabilidades, causas o amenazas y riesgos frente a cada activo de la entidad, información que se encuentra en el “ANEXO F: Listado Riesgos, Vulnerabilidades y Amenazas FPS” referenciado en este documento.

3.3.3 Lista de riesgos de seguridad. También se identificaron los riesgos y los activos a los que afectan, el detalle de la Tabla 4 se encuentra en el “ANEXO F: Listado Riesgos, Vulnerabilidades y Amenazas FPS”anexo: Listado Riesgos, Vulnerabilidades y Amenazas FPS.

Tabla 4. Riesgos

Riesgo
Perdida, adulteración o deterioro de la información en medio físico y/o digital
Alteración y destrucción de la información en las bases de datos
No cumplimiento de normas, reglamentos, acuerdos y políticas de seguridad de la información
Ataques a la infraestructura tecnológica
No cumplimiento y seguimiento a los acuerdos de confidencialidad en los contratos de soporte y mantenimiento de los sistemas de información
Fallas en el proceso de copia de respaldo de los procesos
No obtener información correcta hacia los procesos en el tiempo preciso para la toma de decisiones apropiadas.
Perdidas de bienes o activos fijos del Fondo de Pasivo Social FNC
Acceso no autorizado a los sistemas de información, aplicaciones
Uso inapropiado por parte de los funcionarios en el manejo de la información contenida en los sistemas de información del Fondo
Información confidencial o sensible quede en disposición de personas que no tiene la autorización apropiada para obtener acceso
Sustracción de los expedientes historias laborales de extrabajores y/o pensionados, y de beneficiarios al sistema de salud o documentos para beneficios mal intencionados
Ausencia de estrategias y/o planes de continuidad de negocio
Ausencia de protocolos de seguridad de la información financiera
Violación de derechos de autor
Obsolescencia de los activos tecnológicos
Uso inapropiado por parte de los funcionarios en el manejo de la información contenida en los sistemas de información del Fondo

Tabla 4. (Continuación)

Riesgo
Información confidencial o sensible quede en disposición de personas que no tiene la autorización apropiada para obtener acceso
Sustracción de los expedientes historias laborales de extrabajores y/o pensionados, y de beneficiarios al sistema de salud o documentos para beneficios mal intencionados
Ausencia de estrategias y/o planes de continuidad de negocio
Ausencia de protocolos de seguridad de la información financiera
Violación de derechos de autor
Obsolescencia de los activos tecnológicos
Fuente: Autores

3.3.4 Evaluación de riesgos (Probabilidad/impacto). Respecto a la evaluación del riesgo, se hizo un análisis basado en el "ANEXO C: Guía metodológica de análisis de riesgos de seguridad y privacidad de la información FPS" que se encuentra referenciado en este documento, el cual incluye la identificación, análisis y evaluación de los riesgos presentes en los procesos de la entidad, que apoyados en criterios previamente expuestos por los líderes de cada proceso permiten medir la probabilidad e impacto de cada riesgo en caso de que se materialicen, esto a su vez permite ser una base para la toma de decisiones de la entidad frente a los riesgos encontrados y de esta manera enfocar los esfuerzos en el tratamiento de los mismos, este análisis se encuentra en el "ANEXO F: Listado Riesgos, Vulnerabilidades y Amenazas FPS" referenciado en este documento.

3.3.5 Lista de riesgos priorizados. El listado de riesgos priorizados obtenido de forma posterior a la evaluación de riesgos del "ANEXO F: Listado Riesgos, Vulnerabilidades y Amenazas FPS", de donde se seleccionaron aquellos riesgos que se encuentran en una zona de riesgo alta (Reducir el Riesgo, Evitar, Compartir o Transferir el Riesgo) o extrema (Reducir el Riesgo, Evitar, Compartir o Transferir el Riesgo) después de aplicados los controles.

A continuación se muestra en el Cuadro 9, el listado de riesgos priorizados.

Cuadro 9. Listado riesgos priorizados

Zona	Riesgo
Alta	Acceso no autorizado a los sistemas de información, aplicaciones debido a que políticas de contraseñas no seguras afectando la disponibilidad, integradas y confidencialidad de la información,
	Información confidencial o sensible quede en disposición de personas que no tiene la autorización apropiada para obtener acceso
	Violación de derechos de autor
	Obsolescencia de los activos tecnológicos
Extrema	Alteración y destrucción de la información en las bases de datos
	Ataques a la infraestructura tecnológica
	Interrupción total o parcial en la plataforma tecnológica del Fondo , debido a la ausencia de estrategias y/o planes de continuidad de negocio afectando la Disponibilidad de la información
Fuente: Autores	

3.3.6 Declaración de aplicabilidad. Dentro de los requerimientos de la ISO 27001:2013, se encuentra la declaración de aplicabilidad, por lo cual se creó el "ANEXO J: Declaración de Aplicabilidad" referenciado en este documento y que hace mención de todos los controles que hacen parte de la norma en cuestión, así como los objetivos de cada uno y su aplicabilidad a la entidad. Al ser una información tan extensa, se omito su colocación dentro de este documento y se recomienda dirigirse al anexo antes mencionado para ver su detalle.

3.4 PLANES DE TRATAMIENTO DE RIESGOS

Con el objetivo de gestionar el riesgo residual se establecieron los planes de tratamiento del riesgo, orientados a garantizar la confidencialidad, integridad y disponibilidad de los activos de información de la entidad.

Para determinar la opción para el tratamiento del riesgo, se utilizó como base el "ANEXO C: Guía metodológica de análisis de riesgos de seguridad y privacidad de la información FPS" que se encuentra referenciado en este documento, donde dependiendo del desplazamiento o no que generaron los controles recomendados, se encontraron los planes de tratamiento enfocados en evitar, disminuir o mitigar el riesgo residual.
A continuación se muestran en el Cuadro 10 aquellas medidas de respuesta frente a los riesgos identificados, cuyo mayor detalle se encuentra en el "ANEXO F: Listado Riesgos, Vulnerabilidades y Amenazas FPS".

Cuadro 10. Planes de tratamiento de riesgo

Riesgo	Nivel Riesgo	Medidas de Respuesta	Acciones	Responsable
Perdida , adulteración o deterioro de la información en medio físico y/o digital	Zona De Riesgo Baja	Asumir el Riesgo	P: Diagnostico general del estado de la gestión documental H: Elaboración del programa de gestión documental V: Implementación del programa de gestión documental A: seguimiento del programa de gestión documental	Gestión Documental / Gestión Tic's
Alteración y destrucción de la información en las bases de datos	Zona De Riesgo Extrema	Reducir el Riesgo, Evitar, Compartir o Transferir el Riesgo	P: Revisar los procedimientos de APGTSOPSPT06 creación, modificación y eliminación de usuarios en el sistema, APGTSOPSPT07 Mantenimiento de servidor de aplicaciones y base datos H: Modificar los procedimiento colocando puntos de control V: Aprobación de los procedimiento ante el comité de control interno y calidad A: Socialización de los procedimiento a los funcionarios de la entidad	Gestión Tic's
No cumplimiento de normas, reglamentos, acuerdos y políticas de seguridad de la información	Zona De Riesgo Baja	Asumir el Riesgo	P: Cronograma de jornada H: Por medio de miércoles de seguridad. V: Encuesta para medir el impacto generado A: Incluir campaña de contraseñas, escritorio limpio y medios removibles , políticas de seguridad y privacidad de información , el buen uso de los equipos de buenas prácticas de seguridad en el plan institucional	Gestión Tic's
Ataques a la infraestructura tecnológica	Zona De Riesgo Extrema	Reducir el Riesgo, Evitar, Compartir o Transferir el Riesgo	P: Diseño de un plan de estudio para infraestructura tecnológica H: Elaboración de estrategia de protección para la infraestructura tecnológica V: Seguimientos a los controles establecidos en la estrategia A: Seguimiento al cumplimiento de la estrategia	Gestión Tic's

Cuadro 10.(Continuación)

Riesgo	Nivel Riesgo	Medidas de Respuesta	Acciones	Responsable
No cumplimiento y seguimiento a los acuerdos de confidencialidad en los contratos de soporte y mantenimiento de los sistemas de información	Zona De Riesgo Moderada	Asumir el Riesgo, Reducir el Riesgo	P: Definir y establecer la política e información completa sobre aspectos relevantes para la contratación de servicios H: .Introducir estos aspectos establecidos dentro de los contratos V: Verificar del cumplimiento A: Notificar del seguimiento a través de informe de cumplimiento	Gestión Tic's/Asistencia Jurídica Gestión Bienes Transferidos / Gestión De Servicios Administrativos / Gestión De Talento Humano
Fallas en el proceso de copia de respaldo de los procesos debido a que no se puede acceder al respaldo ni a la recuperación de la información de contingencia afectando Disponibilidad de la información.	Zona De Riesgo Moderada	Asumir el Riesgo, Reducir el Riesgo	P: Definir el alcance del Plan de Continuidad del Negocio de los servicios del Fondo. H: Elaboración de los planes relacionados con el Plan de Continuidad del Negocio de los servicios de del Fondo. V: Validación y revisión de los documentos elaborados por parte de la dirección. A: Adquisición y ejecución de lo establecido en los planes relacionados con el Plan de Continuidad del Negocio de los servicios de del Fondo.	Gestión Tic's
No obtener información correcta hacia los procesos en el tiempo preciso para la toma de decisiones apropiadas.	Zona De Riesgo Moderada	Asumir el Riesgo, Reducir el Riesgo	P: Diagnostico del estado de la UPS, Red eléctrica y Firewall H: Mantenimiento de las UPS, Red eléctrica y actualización del Firewall V: Pruebas de Funcionamiento y penetración A: Realizar la reposición de la UPS E inclusión de reglas para el Firewall	Gestión Tic's
Perdidas de bienes o activos fijos del Fondo de Pasivo Social FNC	Zona De Riesgo Baja	Asumir el Riesgo	P: Elaborar Inspección de los controles establecidos cámaras software de inventario y sistemas de vigilancia H: Ejecutar el plan para optimizar rendimiento del controles cámaras software de inventario y sistemas de vigilancia. V: Realizar seguimiento del controles cámaras software de inventario y sistemas de vigilancia. . A: Realizar informe de resultados de las mejoras implementadas y su impacto.	Gestión Bienes Transferidos / Gestión De Servicios Administrativos

Cuadro 10. (Continuación)

Riesgo	Nivel Riesgo	Medidas de Respuesta	Acciones	Responsable
Uso inapropiado por parte de los funcionarios en el manejo de la información contenida en los sistemas de información del Fondo	**Zona De Riesgo Moderada**	**Asumir el Riesgo, Reducir el Riesgo**	P: Cronograma de jornada H: Por medio de miércoles de seguridad. V: Encuesta para medir el impacto generado A: Incluir campaña de contraseñas, escritorio limpio y medios removibles , políticas de seguridad y privacidad de información , el buen uso de los equipos de buenas prácticas de seguridad en el plan institucional	Gestión Tic's
Uso inapropiado por parte de los funcionarios en el manejo de la información contenida en los sistemas de información del Fondo	**Zona De Riesgo Moderada**	**Asumir el Riesgo, Reducir el Riesgo**	P: Cronograma de jornada H: Por medio de miércoles de seguridad. V: Encuesta para medir el impacto generado A: Incluir campaña de contraseñas, escritorio limpio y medios removibles , políticas de seguridad y privacidad de información , el buen uso de los equipos de buenas prácticas de seguridad en el plan institucional	Gestión Tic's
Información confidencial o sensible quede en disposición de personas que no tiene la autorización apropiada para obtener acceso	**Zona De Riesgo Alta**	**Reducir el Riesgo, Evitar, Compartir o Transferir el Riesgo**	P: Elaborar Inspección de los controles establecidos cámaras software de inventario y sistemas de vigilancia H: Ejecutar el plan para optimizar rendimiento del controles cámaras software de inventario y sistemas de vigilancia. V: Realizar seguimiento del controles cámaras software de inventario y sistemas de vigilancia. . A: Realizar informe de resultados de las mejoras implementadas y su impacto.	Gestión Bienes Transferidos / Gestión De Servicios Administrativos
Sustracción de los expedientes historias laborales de extrabajores y/o pensionados, y de beneficiarios al sistema de salud o documentos para uso mal intencionados	**Zona De Riesgo Baja**	**Asumir el Riesgo**	P: Diagnostico general del estado de la gestión documental H: Elaboración del programa de gestión documental V: Implementación del programa de gestión documental A: seguimiento del programa de gestión documental	Gestión Documental / Gestión Tic's
Interrupción total o parcial en la plataforma tecnológica del Fondo , debido a la ausencia de estrategias y/o planes de continuidad de negocio afectando la Disponibilidad de la información	**Zona De Riesgo Extrema**	**Reducir el Riesgo, Evitar, Compartir o Transferir el Riesgo**	P: Definir el alcance del Plan de Continuidad del Negocio de los servicios del Fondo. H: Elaboración de los planes relacionados con el Plan de Continuidad del Negocio de los servicios de del Fondo. V: Validación y revisión de los documentos elaborados por parte de la dirección. A: Adquisición y ejecución de lo establecido en los planes relacionados con el Plan de Continuidad del Negocio de los servicios de del Fondo.	Gestión Tic's

Cuadro 10. (Continuación)

Riesgo	Nivel Riesgo	Medidas de Respuesta	Acciones	Responsable
Ausencia de protocolos de seguridad de la información financiera	**Zona De Riesgo Baja**	**Asumir el Riesgo**	P: Identificar protocolos existentes para mirar la viabilidad de modificación H: Ejecutar pruebas de efectividad V: Elaboración de informe de evaluación de los protocolos A: Con base en los resultados del informe evaluación de los protocolos determinar eficacia de los protocolos planteadas y estudiar la posibilidad de actualizarlos, modificarlos y/o reemplazarlos	Recursos Financieros
Violación de derechos de autor	**Zona De Riesgo Alta**	**Reducir el Riesgo, Evitar, Compartir o Transferir el Riesgo**	P: Establecer reglas para la instalación de software por parte de los funcionarios H: Socializar al interior de la entidad V: verificar el cumplimiento a través de la herramienta de PC SECURE A: Realizar informe de la acciones tomadas	Gestión Tic's
Obsolescencia de los activos tecnológicos	**Zona De Riesgo Alta**	**Reducir el Riesgo, Evitar, Compartir o Transferir el Riesgo**	P: Contar con un contrato de manteamiento preventivo, correctivo y soporte técnico de los equipos de la entidad. H: Realizar ficha técnica y estudio de mercado para el contrato de mantenimiento y soporte de los equipos de la entidad. V: Realizar ficha, estudio de mercado, estudios previos y validarlo con Contratación para iniciar proceso licitatorio. . A: Adquisición del servicio	Gestión Bienes Transferidos / Gestión De Servicios Administrativos
Fuente: Autores				

3.5 DOCUMENTACIÓN DEL SGSI

3.5.1 Políticas específicas de seguridad a adoptar

3.5.1.1 Política de estructura organizacional de seguridad de la información. El Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia establecerá un esquema para la seguridad de la información que cuente con roles y

responsabilidades definidas que consideren actividades como la operación gestión y administración de la seguridad de la información en la entidad.

A continuación se establecen las medidas de la política de estructura organizacional de seguridad de la información del Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia:

- La Alta Dirección Del Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia debe definir y establecer las respectivas responsabilidades y roles relacionados con la seguridad de la información.

- La Alta Dirección debe revisar y aprobar las Políticas de Seguridad de la Información que han sido definidas en este documento.

- La Alta Dirección debe promover dentro de la entidad, una cultura de seguridad de la información de forma activa y permanente.

- La Alta Dirección debe facilitar la socialización de las Políticas de Seguridad de la información a todo el personal de la entidad.

- La Alta Dirección, debe asignar los recursos, la infraestructura y el personal que sea necesario para la gestión correcta de la seguridad de la información del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA.

- El Comité de Seguridad de la Información o el que haga sus veces, debe revisar, actualizar y presentar ante la alta dirección las Políticas de Seguridad de la Información, la metodología para la gestión del riesgo, la clasificación de la información, y demás temas relacionados.

- El Comité de Seguridad de la Información o el que haga sus veces, debe analizar los incidentes de seguridad que le sean escalados y realizar el debido proceso de contacto con las autoridades en caso de ser necesario.

- El Comité de Seguridad de la Información o el que haga sus veces, debe constatar que se cumplan las políticas de seguridad de la información mencionadas en este documento.

- La Oficina de Control Interno o la que haga sus veces, debe planificar y ejecutar las auditorías internas al Sistema de Gestión de Seguridad de la Información del Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia con el fin de determinar si las políticas, procedimientos, controles y procesos establecidos están acordes con los requerimientos de la entidad en cuanto a institucionalidad, seguridad y regulaciones aplicables.

- La Oficina de Control Interno o la que haga sus veces, debe realizar revisiones parciales y totales de todos los procesos o áreas que hagan parte del alcance del Sistema de Gestión de Seguridad de la Información de la entidad, de manera que pueda de verificar la eficacia de las acciones preventivas y correctivas que se realicen.

- La Oficina de Control Interno o la que haga sus veces debe informar a las personas y áreas responsables cuando se encuentren hallazgos durante las auditorias.

- El proceso Gestión TIC´S debe asignar los roles, responsabilidades y funciones al personal que se requiera para la operación y administración del Sistema de Gestión de Seguridad de la Información, donde esto debe estar debidamente documentado y segregado.

3.5.1.2 Política para uso de conexiones remotas. El Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia establecerá las circunstancias y requisitos bajo las cuales se permitirá el establecimiento de conexiones remotas a la plataforma tecnológica de la entidad; Del mismo modo, facilitará las herramientas necesarias para garantizar que dichas conexiones se realicen de forma segura.

A continuación se establecen las medidas de la política para uso de conexiones remotas Del Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia:

- El proceso Gestión TIC´S debe revisar y aprobar los métodos de conexión remota a la plataforma tecnológica de la entidad.

- El proceso Gestión TIC´S debe restringir las conexiones remotas; permitiendo únicamente que estas se realicen por personal autorizado y por lapso de tiempo previamente establecidos, de acuerdo con la labor a desempeñarse durante la conexión.

- El proceso Gestión TIC´S debe validar la efectividad de los controles aplicados sobre las conexiones remotas de forma permanente.

- La Oficina de Control Interno debe, dentro de su autonomía, realizar las respectivas auditorías sobre los controles implantados para las conexiones remotas de la entidad.

- Los usuarios que realicen conexión remota deben tener las aprobaciones requeridas para establecer dicha conexión y siempre deben respetar las condiciones de uso establecidas para las conexiones.

- Los usuarios únicamente deben establecer conexiones remotas en equipos identificados previamente, evitando en todo momento el uso de computadores públicos, cafés internet y demás similares.

3.5.1.3 Política de seguridad del personal. El Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia reconoce la importancia que tiene el recurso humano para el logro de los objetivos de la entidad, por tal razón y con el fin de contar con personal altamente calificado, garantizará que la vinculación de funcionarios se realice bajo un proceso formal de selección, acorde con la legislación vigente.

A continuación se establecen las medidas de la política de seguridad del personal del Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia:

- La Oficina Asesora Jurídica y el proceso Gestión de Talento Humano deben realizar las verificaciones que se requieran para confirmar la veracidad de la información que sea suministrada por el posible personal a ocupar un cargo en El

Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia, antes de realizar cualquier vinculación con el mismo.

- La Oficina Asesora Jurídica y el proceso Gestión de Talento Humano deben garantizar que los funcionarios de la entidad firmen un Acuerdo y/o Cláusula de Confidencialidad así como un documento de Aceptación de Políticas de Seguridad de la Información; estos documentos deben ser adjuntos a los demás documentos relacionados con la vinculación del personal.

- Cada Supervisor de Contrato, jefe inmediato y/o similar debe constatar la existencia de Acuerdos y/o Cláusulas de Confidencialidad así como del documento de Aceptación de Políticas de Seguridad de la Información antes de dar cualquier acceso a la información del Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia.

- El personal provisto por terceros para realizar labores en o para el Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia debe firmar un Acuerdo y/o Cláusula de Confidencialidad y el documento de Aceptación de Políticas de Seguridad de la Información, antes de que se les facilite cualquier acceso a las instalaciones y a la plataforma tecnológica de la entidad.

3.5.1.4 Política de desvinculación, licencias, cambio de labor, vacaciones de personal y contratistas. El Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia, garantizara que su personal, y contratistas sean desvinculados o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura.

A continuación se establecen las medidas de la política de desvinculación, licencias, cambio de labor o vacaciones de personal y contratistas del Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia:

- El proceso Gestión de Talento Humano debe realizar el proceso de desvinculación, licencias, cambio de labor, vacaciones de personal y contratistas de la entidad, realizando los procedimientos y controles establecidos para dicha finalidad.

• Cada Supervisor de Contrato, Jefe de Oficina o similar, debe monitorear y reportar de manera inmediata la desvinculación o cambio de labores de personal o contratistas de la entidad tanto al proceso Gestión de TIC´S quien realizará la modificación o inhabilitación de usuarios.

3.5.1.5 Política de uso de medios de almacenamiento y periféricos. El uso de medios de almacenamiento y periféricos en los recursos de la plataforma tecnológica del De Pasivo Social De Ferrocarriles Nacionales De Colombia será estipulado por el proceso Gestión de TIC´S considerando las labores que realice el personal y las necesidades respectivas.

A continuación se establecen las medidas de la política de uso de medios de almacenamiento y periféricos del Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia:

• El proceso Gestión TIC´S en conjunto con el comité de Seguridad de la Información o el que haga sus veces, deben establecer las condiciones para el uso de medios de almacenamiento y periféricos dentro de la plataforma tecnológica del Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia.

• El proceso Gestión TIC´S debe estipular y aplicar el proceso para la disposición segura de los medios de almacenamiento de la entidad cuando estos sean dados de baja o re-asignados a otro usuario.

3.5.1.6 Política de acceso a redes y recursos de red. El proceso Gestión TIC´S, como responsables de las redes de datos y los recursos de red del Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia, debe buscar que las redes sean protegidas de manera adecuada contra accesos no autorizados a través de mecanismos de control de acceso.

A continuación se establecen las medidas de la política de acceso a redes y recursos de red del Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia:

• El proceso Gestión TIC´S debe establecer un procedimiento y unos debidos controles para proteger el acceso tanto a las redes de datos como a los recursos de red de la entidad.

- El proceso Gestión TIC´S bajo la supervisión de los líderes de procesos, debe autorizar la creación y/o modificación de las cuentas de acceso a las redes o recursos de red del Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia.

- El proceso Gestión TIC´S debe verificar de forma periódica todos los controles de acceso a los recursos de red y servicios de la plataforma de la entidad.

- Los equipos que se conecten o deseen conectarse a las redes de datos de la entidad, deben cumplir con los requisitos o controles dispuestos para ello, y solo podrán realizar las tareas para las que fueron autorizados.

3.5.1.7 Política de control de acceso. El proceso Gestión TIC´S debe controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática.

A continuación se establecen las medidas de la política de control de acceso del Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia:

- Las claves y contraseñas asignadas a cada funcionario son de carácter personal e intransferible, su uso debe ser de manera responsable, tener un buen manejo, efectuar cambios de manera periódica y por seguridad deben ser alfanumérica de mínimo 8 caracteres e incluir Mayúsculas y minúsculas; No se permite el préstamo de claves y contraseñas.

- Los funcionarios al abandonar temporalmente su puesto de trabajo deben bloquear sus sesiones y al finalizar la jornada laboral o cuando exista ausencia temporal que supere dos (2) horas deberán apagar sus equipos o estaciones de trabajo.

- El oficial de seguridad de la información deber establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información, los cuales debe comprender todas las fases del ciclo de vida del acceso del usuario, desde el registro inicial de los usuarios nuevos hasta la

cancelación final del registro de usuarios que ya no requieren acceso a los servicios y sistemas de información.

- Todos los funcionarios, contratista del fondo deben mantener controles de accesos eficientes, en particular con relación al uso de contraseñas, a la seguridad del equipo del usuario, al de tener conservar escritorio y pantalla despejados para reducir el riesgo de acceso no autorizado o daño de reportes, medios y servicios de procesamiento de Información.

- El proceso Gestión de TIC´S debe asegurar el bloqueo al acceso de páginas de contenido para adultos, redes sociales, hacking, descargas (FTP), mensajería instantánea y cualquier página que represente riesgo potencial para la Entidad mediante el uso de servidor proxy, firewall o el software que mejor se ajuste a la necesidad. Excepciones de acceso, serán aprobados por el jefe inmediato, según la necesidad del cargo y verificación previa de que las paginas solicitadas no contengan código malicioso con el visto bueno del oficial de seguridad de la información.

- El acceso a los sistemas operativos de la entidad deben estar protegidos por registros de inicio seguro, contemplando las siguientes condiciones no mostrar información del sistema, hasta que el proceso de inicio se haya completado, no suministrar mensajes de ayuda, durante el proceso de autenticación, validar los datos de acceso, una vez que se han diligenciado todos los datos de entrada, limitar el número de intentos fallidos de conexión auditando los intentos no exitosos, no mostrar las contraseñas digitadas, No transmitir la contraseña en texto claro.

- El uso de programas utilitarios debe ser limitado y minuciosamente controlado por el oficial de seguridad de la información con el objeto de garantizar la instalación de software no autorizado y cambios de configuración del sistema.

3.5.1.8 Política de Seguridad Física y del Entorno. El Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia implementara y velara por la efectividad de los mecanismos de seguridad tanto físicos como de control de acceso, que permitan asegurar el perímetro de las instalaciones, a la vez que controlen las amenazas físicas tanto internas como externas y las condiciones de medio ambiente que se puedan presentar en las oficinas de la entidad.

A continuación se establecen las medidas de la política de Seguridad Física y del Entorno del Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia:

- Garantizar la protección del perímetro de seguridad de las instalaciones físicas.

- Controlar el acceso a áreas restringidas tales como infraestructura de soporte de los sistemas de información**.**

- Todos los funcionarios , contratista y visitantes o terceras personas, que ingresen a las instalaciones del Fondo de Pasivo Social deberán poseer una identificación a la vista que claramente los identifique como tal.

3.5.1.9 Política de Gestión de Activos. Los procesos de la entidad con el acompañamiento y asesora del Gestión TIC´S, deben, establecer la forma de identificación, uso, administración y responsabilidad frente a los activos de Información, con el fin de cumplir con los siguientes objetivos:

- Garantizar que los activos de información reciban un apropiado nivel de protección. Clasificar la información para señalar su criticidad, sensibilidad y reserva de la misma.

- Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

A continuación se establecen las medidas de la política de gestión de activos del Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia:

- Identificar los activos de información de acuerdo a su tipo, su criticidad, sensibilidad y reserva de la misma, los cuales deben ser documentados y mantenidos actualizados, además de definir las funciones que deberán tener permisos de acceso a la información los responsables, los propietarios de la información o conocedor de los mismos dentro de la entidad centralizado por el proceso de gestión de TIC´S.

- El dueño o propietario de los activos de información, será el responsable de definir la categoría en la que cada activo de información se encuentra, así como determinar si es necesario un proceso de reclasificación y los controles requeridos para su protección.

- El uso de los activos de información pertenecientes al Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia es de responsabilidad del propietario asignado; es su deber proteger y mantener la confidencialidad, integridad y disponibilidad de los activos de información.

- Establecer los criterios y niveles de calificación de la información, para definir las medidas de protección adecuadas de los activos. Estos criterios se determinan de acuerdo con la confidencialidad, declarados en la ley 1712 del 2014 y la ley 1581 de 2012:

INFORMACION PÚBLICA RESERVADA: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley.

Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.

INFORMACION PÚBLICA CLASIFICADA: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley.

Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma.

Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.

INFORMACION PÚBLICA: Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.

Es aquella que puede ser accedida por cualquier persona, incluso por personas o entidades externas a la organización, con o sin vínculos laborales, comerciales, legales, entre otros.

NO CLASIFICADA: Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información.

DATO PÚBLICO: "Calificado como tal en la ley. Dato que no es semiprivado, privado o sensible (Ej. Datos relativos al estado civil de las personas, su profesión u oficio, su calidad de comerciante o servidor público y aquellos que pueden obtenerse sin reserva alguna)."

DATO SEMIPRIVADO: Dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento interesa al titular y a cierto sector o grupo de personas o a la sociedad en general (Ej. Datos financieros y crediticios, dirección, teléfono, correo electrónico).

DATO PRIVADO: Dato que solo es relevante para su titular (Ej. Fotografías, videos, datos relacionados con su estilo de vida.)

DATO SENSIBLE: Categoría especial de datos personales. Se consideran datos sensibles aquellos datos referidos a ideología, creencias, religión, afiliación sindical, salud, origen racial o vida sexual de las personas.

Su criticidad

De acuerdo a las siguientes categorías:

Confidencialidad: Donde su valoración es alta si es información reservada, media en caso de que sea clasificada y baja si es pública.

Integridad: Donde su valoración será alta en caso de que sea información sea crítica o no crítica.

Disponibilidad: donde la valoración es alta, media o baja de acuerdo a su criticidad.

- Cada activo de información serán etiquetados de acuerdo con el esquema de clasificación aprobado por la entidad y teniendo en cuenta las tablas de retención documental establecidas en cada proceso.

- Definir un procedimiento para el etiquetado y manejo de la información de con el esquema de clasificación y teniendo en cuenta la tablas de retención documental establecidas en cada proceso el cual debe ser aprobado por la entidad.

3.5.1.10 Política de Seguridad de la información en la Continuidad de las tecnologías de la información. El proceso Gestión TIC´S y los responsables del tema de Seguridad de la información deben contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos frente a fallas, ataques o desastres**.**

A continuación se establecen las medidas de la política de seguridad de la información en la continuidad de las tecnologías de la información del Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia:

- Seguir con la estrategia de recuperación establecida en el plan de contingencia de las tecnologías de la información y las comunicaciones (TIC), para asegurar la restauración de los procesos críticos del negocio, ante el evento de una contingencia.

- Contar con instalaciones alternas y con capacidad de recuperación, que permitan mantener la continuidad del negocio aún en caso de desastre en las instalaciones de los lugares de operación.

• Incluir los controles establecidos en cada una del proceso que se clasificaron críticos, para que no se vean disminuidos los aspectos de seguridad en caso de desastre.

3.5.1.11 Política de protección frente a software malicioso. El Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia proporcionará los mecanismos necesarios para garantizar la protección de la información y recursos de la plataforma tecnológica en donde almacena, procesa su información y la de sus afiliados, adoptando los controles que sean necesarios para evitar la modificación, daño o divulgación ocasionada por el contagio de software malicioso.

A continuación se establecen las medidas de la política de protección frente a software malicioso del Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia:

• El proceso Gestión TIC´S debe proveer herramientas tales como software antivirus, antimalware, antispam, antispyware y demás (con las respectivas licencias de uso requeridas), que permitan reducir el riesgo de contagio de software malicioso y que a su vez respalden la seguridad de la información que se encuentra administrada y almacenada en la plataforma de la entidad.

• El proceso Gestión TIC´S, a través de su equipo de trabajo, debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de protección de software malicioso.

• Los usuarios deben asegurarse que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras.

• Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar al proceso Gestión TIC´S para que se tomen las medidas correspondientes.

3.5.1.12 Política de copias de respaldo de la información. Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia garantizará la realización de copias

de seguridad donde se respalde y almacene la información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades, adicionalmente, el proceso Gestión TIC´S, velará porque los medios magnéticos donde se almacene la información crítica, se encuentren en una ubicación distinta a las instalaciones donde se encuentra dispuesta, ubicación que debe contar con los controles de seguridad física y ambiental adecuados.

A continuación se establecen las medidas de la política copias de respaldo de la información del Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia:

- El proceso Gestión TIC´S, a través de su equipo de trabajo debe generar y adoptar los procedimientos para el almacenamiento, generación, restauración y tratamiento de las copias de seguridad y respaldo de la información, buscando garantizar su integridad y disponibilidad.

- Es responsabilidad de los usuarios de la plataforma tecnológica de la entidad, el identificar la información considerada como crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

3.5.1.13 Política de gestión de vulnerabilidades. El Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia través del proceso Gestión TIC´S revisará de forma periódica la aparición de vulnerabilidades técnicas sobre los recursos de la entidad por medio de la realización periódica de pruebas de vulnerabilidades.

A continuación se establecen las medidas de la política de gestión de vulnerabilidades del Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia:

- El proceso Gestión TIC´S debe revisar de forma periódica la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la respectiva plataforma así como de los administradores de los sistemas de información con el fin de prevenir la exposición al riesgo de estos.

- El proceso Gestión TIC´S a través de su equipo de trabajo debe generar y ejecutar o monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica de la entidad.

3.5.1.14 Política para el tratamiento de datos personales. En cumplimiento de la de Ley 1581 de 2012y su decreto reglamentario, por la cual se dictan disposiciones para la protección de datos personales, el Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia, como custodio, responsable y/o encargado del tratamiento de datos personales, garantizará la protección de los datos personales de sus afiliados, proveedores y/o terceros recibida a través de los diferentes canales de recolección de información y hará uso de los mismos únicamente para las finalidades para las que se encuentra facultado, especialmente las señaladas a continuación:

- Reconocer las prestaciones económicas y ordenar el respectivo pago.

- Para el reporte de estadísticas que alimentan el sistemas de salud a los entes rectores y de control como Ministerio de Salud y Protección Social, Supersalud - Superintendencia Nacional de Salud, Secretarias de Salud.

- Para los fines administrativos propios de la entidad.

- Para la administración y prestación de los servicios de salud a los obligados a prestar dicho servicio.

- Caracterizar ciudadanos y grupos de interés y adelantar estrategias de mejoramiento en la prestación del servicio.

- Dar tratamiento y respuesta a las peticiones, quejas, reclamos, denuncias, sugerencias y/o felicitaciones presentados a la entidad.

- Alimentar el Sistema de Información y Gestión de Empleo Público –SIGEP.

- Asuntos jurisdiccionales.

DEBERES DEL RESPONSABLE DEL TRATAMIENTO

Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

- Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

- Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular.

- Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.

- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.

- Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.

- Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.

- Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley.

- Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.

- Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley.

- Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos.

- Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.

- Informar a solicitud del Titular sobre el uso dado a sus datos.

- Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

- Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

A continuación se establecen las medidas de la política de protección de datos personales del Fondo De Pasivo Social De Ferrocarriles Nacionales De Colombia:

- El fondo realiza el tratamiento de Datos Personales en ejercicio propio de sus funciones legales y para el efecto no requiere la autorización previa, expresa e informada del Titular. Sin embargo, cuando no corresponda a sus funciones deberá obtener la autorización por medio de un documento físico, electrónico, mensaje de datos, Internet, sitio web, o también de manera verbal o telefónica o en cualquier otro formato y mantendrá las pruebas de ésta para su posterior consulta.

- Los Datos Personales que hayan sido sometidos a Tratamiento deberán ser exacto, completo, veraz, actualizado, comprobable y comprensible. El fondo conservará la información bajo estas características siempre y cuando el titular informe oportunamente sus novedades y serán tratados por aquellos Funcionarios del Fondo que cuenten con el autorización para ello, o quienes dentro de sus funciones tengan a cargo la realización de tales actividades o por los Encargados.

- Los datos personales sometidos a Tratamiento se les deben proveer las medidas humanas y técnicas para su protección garantizando su seguridad de que no puedan ser divulgados, modificados accedidos sin previa autorización, eliminados o se entrega terceros sin autorización del titular.

- En caso de delegar a un tercero para el tratamiento de datos personales, la entidad exigirá a este la correcta implementación de lineamientos y procedimientos necesarios para salvaguardar la integridad y protección de los datos personales y garantizar que la información que le suministre sea veraz, completa, exacta, actualizada, comprobable y comprensible. Adicionalmente le comunicará de manera oportuna todas las novedades a que haya lugar para que la información siempre se mantenga actualizada.

- El fondo registra las bases de datos en el Registro Nacional de Base de Datos RNBD – en cumplimiento a los establecido en la ley 1581 de 2012.

- El Titular de los datos personales puede ejercer, principalmente, sus derechos mediante la presentación de consultas y reclamos ante la SIC, en su sede cuyo domicilio es la carrera 13 No. 18 – 24 en el proceso de Atención al Ciudadano y por el correo electrónico quejasyreclamos@fps.gov.co.

- El incumplimiento de la política de tratamiento de datos personales acarreará sanciones contempladas en el código único disciplinario y normas relacionadas.

- El Fondo implementará procedimiento para garantizar el cumplimiento de la política de tratamiento de datos personales.

3.5.2 Procedimientos de seguridad a adoptar. Los procedimientos de seguridad que se mencionan a continuación, permiten que el Fondo de Pasivo Social de Ferrocarriles de Colombia, genere una documentación basada en sus propias características tales como sus activos de información, los servicios que presta y los procesos que delinean su funcionamiento. Esto con el fin de mejorar el manejo en cuanto al tema de seguridad de la información.

Dentro de los procedimientos de seguridad que la entidad va adoptar y que se están dentro del “ANEXO G: Procedimientos FPS” del presente documento y donde se encuentran los siguientes:

- Procedimiento elaboración, ejecución y evaluación del plan institucional de capacitación.

- Procedimiento de inventario, clasificación y etiquetado de activos de información.

- Procedimiento registro hojas de vida contratos.

- Procedimiento proceso vinculación de personal de planta.

- Procedimiento creación, modificación y eliminación de usuarios en el sistema.

- Procedimiento entrega de cargos.

- Procedimiento Copias de seguridad de usuarios y servidores.

- Procedimiento autorización de entrada en horas no laborales.

- Procedimiento baja de bienes muebles por obsolescencia, inservibles o no necesarios para el funcionamiento de la entidad.

- Procedimiento mantenimiento de servidor de intranet.

- Procedimiento mantenimiento de servidor de aplicaciones y base datos.

- Procedimiento transferencias documentales al archivo central.

- Procedimiento para el tratamiento de seguridad en los acuerdos con los proveedores que se estable dentro de los contratos.

- Procedimiento de gestión de incidentes de seguridad de la información.

- No se tiene procedimiento de gestión de la continuidad de negocio pero se tiene un plan de emergencia.

De los anteriores procedimientos descriptos se elaboraron los procedimientos de inventario, clasificación y etiquetado de activos de información y de gestión de incidentes de seguridad de la información y los demás se incorporaron a la declaración de aplicabilidad del SGSI y se modificaron.

4. CONCLUSIONES

- Se encontró que la entidad cuenta con un nivel inicial, debido a que se no cuenta con una identificación de activos ni gestión de riesgos relacionados puntualmente con la seguridad de la información, lo que no permite determinar la criticidad de la información que se maneja y por tanto los controles que se tienen en el momento de realizar el diagnostico, no están alineados con el objeto de preservar la integridad, disponibilidad y confidencialidad de la información.

- La mayor parte de organizaciones, no concibe la seguridad de la información como un tema clave para el logro de sus objetivos empresariales, y mucho menos como un pilar clave en sus procesos organizacionales, sin embargo la entidad se ha reconocido esto es fundamental, que al no contar con ello existe un problema y que hay que tratarlo.

- La entidad no cuenta con procesos estandarizados y la implementación de los controles existentes depende de cada individuo, siendo principalmente reactiva y no preventiva.

- La calificación actual de la entidad con relación a los controles del Anexo de la norma ISO 27001:2013, es de 23%, lo que significa que se requiere de un importante esfuerzo de la entidad para cumplir con los requerimientos de la norma ISO 27001:2013 y por consiguiente lo relacionado a la estrategia de gobierno en línea (estrategia GEL) en cuanto al eje de Seguridad y privacidad de la información.

- Se identificaron una serie de vulnerabilidades y amenazas bastante importantes, entre las que sobresalen el acceso no autorizado a los sistemas de información, obsolescencia de activos tecnológicos, alteración y destrucción de la información en las bases de datos, violación de derechos de autor, ataques a la infraestructura tecnológica, interrupción total o parcial en la plataforma tecnológica del Fondo, debido a la ausencia de estrategias y/o planes de continuidad de negocio entre otros.

- Para la metodología de evaluación y tratamiento de riesgo se definió la importancia de realizar un análisis inicial relacionado con el estado actual de la estructura de

riesgo y gestión en la entidad, desde un punto de vista estratégico aplicando la metodología establecida en el presente proyecto.

- Dentro del alcance del Sistema de Gestión de Seguridad de la Información del Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia se estableció que este abarcará 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.

- Se ajustó la política general de Seguridad de la Información de la entidad cuyo fin será la disminución en el impacto generado sobre sus activos, 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 y que será adoptada por sus funcionarios, terceros, aprendices, practicantes y proveedores.

- El diseño del modelo de Seguridad y Privacidad de la información propuesto en este proyecto de grado, resulta ser un excelente insumo que permite a la entidad dar un primer paso para el cumplimiento de la normatividad que les rige y ante poder llegar a implementar un adecuado y sustentable Sistema de Gestión de Seguridad de la Información.

5. RECOMENDACIONES

- Es necesario el establecimiento de políticas de seguridad aprobadas por la Alta Dirección, de manera que se garanticen su correcta implementación, cumplimiento y actualización.

- Se requiere la implementación de controles efectivos y acordes, así como el fortalecimiento de los ya existentes, de manera que se asegure tanto la integridad, como la confidencialidad y disponibilidad de la información de la entidad.

- Se debe fomentar la cultura de seguridad dentro de entidad para que todos los funcionarios y las partes interesadas tomen conciencia de que la información es el activo más importante de la entidad y que se le debe garantizar su protección.

- Es necesario que en la entidad se mejoren los mecanismos de control de acceso y retiro de los equipos.

- Es importante que la entidad evalué la vialidad y pertinencia de la implementación de algunos controles del Anexo de la norma ISO 27001:2013 así como la adquisición de herramientas tecnológicas para su cumplimiento.

- Es fundamental, que en la entidad se implemente un mecanismo de monitoreo de logs de eventos de seguridad, con el fin de identificar y gestionar incidentes de seguridad así como hacer seguimiento a las actividades que realizan tanto los usuarios normales como los administradores de plataformas.

- Es importante que se establezca formalmente el cargo de Oficial de Seguridad de la Información y que este cuente con el apoyo de la alta gerencia.

- La entidad cuenta con un procedimiento denominado “Entrega de cargos” que solo se enfoca en el personal de planta lo que no obliga a otro tipo de empleados como contratistas a seguir este procedimiento, lo que asegura que estos empleados los activos de la entidad que estaban bajo su responsabilidad.

- Se requiere el diseño y puesta en marcha de la estrategia de un plan de continuidad de negocio para garantizar las disponibilidad del 100% de los servicios prestados.

- Se recomienda a la entidad, la inclusión de procedimientos para protección de activos, administración de cuentas personales, controles criptográficos, gestión de cambios, protección contra códigos maliciosos, aseguramiento de servicios en la red y adquisición, desarrollo y mantenimiento de software, de los que actualmente carece.

- Es necesario que la Gerencia de TIC revise su capacidad tanto de personal como de equipos y recursos, con el fin de garantizar la correcta implementación de los controles, políticas y procedimientos que se requieren para cerrar las brechas encontradas en el diagnóstico realizado en este proyecto de grado ya que la mayoría requiere un alto componente tecnológico.

- Es importante que la entidad evalué la viabilidad y pertinencia de algunos controles, políticas y procedimientos debido a que su implementación puede requerir de la adquisición de herramientas tecnológicas de un alto costo y un tiempo de implementación considerable.

- La implementación de dicho SGSI conlleva compromiso y un tiempo prudente y permitirá apalancar desde la Seguridad de la Información, tanto la misión, visión y logro de objetivos de la entidad.

- Por último, se debe garantizar el compromiso de la Alta Directiva hacia la seguridad de la información ya que sin esto, no se recomienda avanzar en el Sistema de Gestión de Seguridad de la Información en ninguna de sus fases.

6. BIBLIOGRAFÍA

AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LAINFORMACIÓN (EINSA). Beneficios, riesgos y recomendaciones para la seguridad de la información. 2009.

ESPINOSA, GARCÍA, GIRALDO. Juan, Rafael, Alexander. Sistema de gestión de seguridad de la información para los tres procesos misionales de la corporación autónoma regional de Risaralda (CARDER). Manizales, 2016, 138 páginas. Trabajo de grado (maestría en gestión y desarrollo de proyectos de software).

GUZMAN, Carlos. Diseño de un Sistema de Gestión de la Seguridad de la Información para una Entidad Financiera de Segundo Piso. Bogotá, 2015, 173 páginas. Trabajo de grado (especialista en seguridad de la información).

ICONTEC. Norma Técnica Colombiana NTC-ISO/IEC 27002 [en línea]. 142 Páginas. 2007.

MINISTERIO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y LAS COMUNICACIONES. Modelo de Seguridad y Privacidad de la Información [en línea]. pág. 9. 2015.

MINISTERIO DE TELECOMUNICACIONES (MINTIC). Modelo de seguridad Gobierno en Línea, Controles de Seguridad y Privacidad de la Información [En línea]. Disponible enhttp://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

--------.-------- Elaboración de la política general de seguridad y privacidad de la información [En línea]. Disponible en http://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

--------.------- Guía de indicadores de gestión para la seguridad de la información [En línea]. Disponible en http://www.mintic.gov.co/gestionti/615/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf

MINISTERIO DE TELECOMUNICACIONES (MINTIC). Modelo de seguridad Gobierno en Línea, Guía de gestión de riesgos [En línea].Disponible en http://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

--------.-------- Guía para la Gestión y Clasificación de Activos de Información [En línea]. Disponible en http://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

--------.------- Guía para la Gestión y Clasificación de Incidentes de Seguridad de la información. [En línea]. Disponible en http://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

-------.------- Modelo de Seguridad y Privacidad de la Información [en línea]. Disponible en http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

--------.-------- Plan de Capacitación, Sensibilización Y Comunicación De Seguridad De La Información [En línea]. Disponible en http://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

--------.-------- Procedimientos De Seguridad De La Información [En línea].Disponible en http://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

--------.------- Roles y Responsabilidades [En línea].Disponible en http://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf

OSORIO, Gustavo. Proyecto de Norma Técnica Colombiana NTC-ISO 27005{En línea} {Fecha de consulta: Agosto 2016}. Disponible enhttps://es.scribd.com/doc/124454177/ISO-27005-espanol

ANEXOS

ANEXO A. Instrumento de evaluación MSPI 2016 FPS

ANEXO B. Política General y Específicas Seguridad de la Información FPS

ANEXO C. Guía metodológica de análisis de riesgos de seguridad y privacidad de la información FPS

ANEXO D. Hoja de Vida Indicadores FPS

ANEXO E. Anexo E. Inventario Activos Datos- Información FPS

ANEXO F. Listado Riesgos, Vulnerabilidades y Amenazas FPS

ANEXO G. Procedimientos FPS

ANEXO H. Reconocimiento Vulnerabilidades Fondo Pasivo Social

ANEXO I.ZAP vulnerabilidades FPS

ANEXO J. Declaración de Aplicabilidad

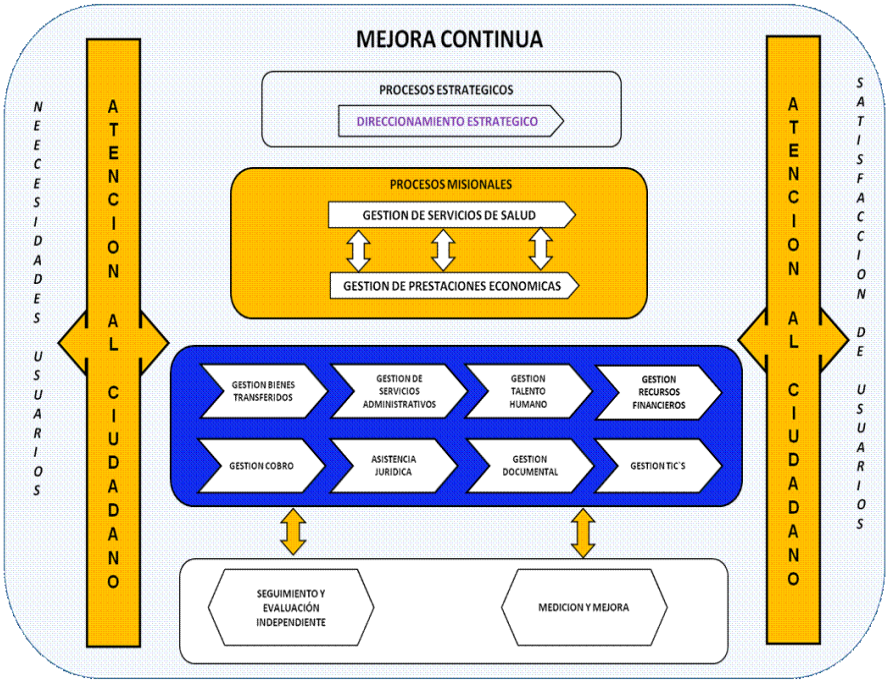
ANEXO A. Instrumento de evaluación MSPI 2016 FPS

Cuadro 1. Datos básicos

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia	vive digital para la gente

DATOS BASICOS	
Tipo Entidad	De orden nacional
Misión	El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia como establecimiento público del orden Nacional, adscrito al Ministerio de Salud y Protección Social, reconoce prestaciones económicas legales y convencionales a los ex trabajadores, pensionados y beneficiarios de las liquidadas empresas Ferrocarriles Nacionales de Colombia y ALCALIS. Así mismo, administramos los servicios de salud a los pensionados y beneficiarios de la empresa liquidada Ferrocarriles Nacionales y Puertos de Colombia. Contamos con la infraestructura tecnológica y el talento humano calificado y comprometido para brindar una excelente prestación de nuestros servicios con calidad y transparencia.
Análisis de Contexto	El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia, es una Empresa del sector público adscrita al Ministerio de la Protección Social, ENTIDAD ADAPTADA DE SALUD EAS que presta servicios de salud a los pensionados de los Ferrocarriles Nacionales de Colombia, Puertos de Colombia y a sus respectivos beneficiarios cuyo misión es reconoce Prestaciones Económicas legales y Convencionales a los ex trabajadores, pensionados y beneficiarios de la liquidada empresa Ferrocarriles Nacionales de Colombia y ALCALIS. Así mismo, de administrar los servicios de salud a los pensionados y beneficiarios de la empresa liquidada Ferrocarriles Nacionales y Puertos de Colombia. OBJETIVOS INSTITUCIONALES Garantizar la prestación de los servicios de salud, que requieran nuestros afiliados a través de la efectiva administración de los mismos. Reconocer las prestaciones económicas y ordenar el respectivo pago. Ser modelo de Gestión Pública en el sector social. Mantener un sistema de información en línea confiable para todos los usuarios del FPS y ciudadanos, que permita una retroalimentación constante. Fortalecer la administración de los bienes de la entidad y la óptima gestión de los recursos. Fortalecer los mecanismos de comunicación organizacional e informativa para proyectar los resultados de la Gestión de la Entidad VISION Dado que contamos con la infraestructura adecuada, recurso humano calificado, experiencia y bajos costos en la prestación de los servicios de reconocimiento y pago de las prestaciones económicas y la administración de servicios de salud con transparencia en la gestión; nuestro reto es consolidarnos como la entidad líder que asuma los compromisos que por mandato legal y/o reglamentario le sean asignados, contribuyendo con las políticas de gestión pública, para el cumplimiento de los fines esenciales del estado en el sector de la seguridad social.

Cuadro 1. (Continuación)

Mapa de procesos	
Organigrama	

Cuadro 1. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia	vive digital para la gente

Preguntas	
¿Qué le preocupa a la Entidad en temas de seguridad de la información?	La protección de la información de los beneficiarios desde el punto de vista de la confidencialidad y la integridad.
¿En qué nivel de madurez considera que está?	En el nivel Inicial
¿En qué componente del ciclo PHVA considera que va?	Planificación

N°	DATOS E INFORMACIÓN A RECOLECTAR PARA LA EVALUACIÓN	NOMBRE DEL DOCUMENTO ENTREGADO	OBSERVACIONES
1	Tipo de entidad (Nacional, Territorial A, Territorial B o C)		Entidad de Orden Nacional.
2	Misión		Se encuentra pública en la intranet y pagina web de la entidad.
3	Análisis de contexto: La entidad debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito y que afectan su capacidad para lograr los resultados previstos en el MSPI.		La entidad para cumplir su propósito a determinado que todos los proceso establecidos en su mapa de proceso son necesarios para logra el resultado provisto en el MSPI.
4	Mapa de Procesos		Se encuentra pública en la intranet de la entidad.
5	Organigrama de la entidad, detallando el área de seguridad de la información o quien haga sus veces		Actualmente la entidad no definido oficialmente el área de seguridad de la información, sin embargo se cuenta con un profesional contratistas de apoyo a la gestión de seguridad de la información desde la oficina Asesora de Planeación y Sistemas.
6	Políticas de seguridad de la información formalizada y firmada	Acto administrativo 2130 de 2014	El fondo cuenta con la Política de Seguridad de la Información aprobado mediante acto administrativo 2130 de 2014 y publica en su intranet; Sin embargo hasta la fecha no ha sido actualizada.
7	Organigrama, roles y responsabilidades de seguridad de la información, asignación del recurso humano y comunicación de roles y responsabilidades.	Acto administrativo 2129 de 2014	Se tiene establecido las responsabilidades de seguridad de la información en el comité anti tramite y gobierno en línea; sin embargo en la actualidad los temas relacionados con este comité se tratan mediante el comité de desarrollo administrativo.

Cuadro 1. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia	vive digital para la gente

N°	Datos e información a recolectar para la evaluación	Nombre del documento entregado	Observaciones
8	Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de la seguridad y privacidad de la información e infraestructura de red de comunicaciones (IPv4/IPv6), revisado y aprobado por la alta dirección.		No se tiene.
9	Documento con el resultado de la herramienta de la encuesta de diagnóstico de seguridad y privacidad de la información, revisado, aprobado y aceptado por la alta dirección.		No se tiene aprobado.
10	Documento con el resultado de la estratificación de la entidad, aceptado y aprobado por la alta dirección.	Borrador en Excel estratificación de la entidad.	La entidad tiene un borrador sin la aprobación de alta dirección.
11	Objetivo, alcance y límites del MSPI (Modelo de Seguridad y Privacidad de la Información).	Borrador en Word Manual de Sistema de Gestión de Seguridad y Privacidad de la Información.	La entidad tiene un borrador sin la aprobación de alta dirección.
12	Procedimientos de control documental del MSPI.		No se tiene.
13	Metodología de Gestión de riesgos.	Borrador en Word incluido en el Manual de Sistema de Gestión de Seguridad y Privacidad de la Información - ESDESDIGGS02 Guía Políticas para la administración del riesgo.	Dentro de la entidad se tiene una metodología general pero no se tiene contemplado los riesgos de seguridad; sin embargo se ha trabaja de manera independiente una metodología que focaliza en los riesgo de seguridad de la información, se recomienda realizar mesas de trabajo para hacer un integral.
14	Riesgos identificados y valorados de acuerdo a la metodología.		No se tiene porque no se ha defino de manera integral la metodología.
15	Planes de tratamiento de los riesgos.		No se tiene porque no se ha defino de manera integral la metodología.
16	Plan y estrategia de transición de IPv4 A IPv6.		No se tiene.
17	Formatos de acuerdos contractuales con empleados y contratistas para establecer responsabilidades de las partes en seguridad de la información.		Dentro de los contratos se tiene una cláusula de confidencialidad que solo garantiza la no divulgación de la información, pero no se tiene establecido de manera específica las responsabilidades de los empleados y contratitas en tema de seguridad de la información.

Cuadro 1. (Continuación)

	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia	
N°	**Datos e información a recolectar para la evaluación**	**Nombre del documento entregado**	**Observaciones**
18	Procedimiento de verificación de antecedentes para candidatos a un empleo en la entidad.	Procedimiento APAJUOAJPT09 Registro hojas de vida y contratos en el SIGEP - APGTHGTHPT07 Procedimiento vinculación de personal e planta.	
19	Documento con el plan de comunicación, sensibilización y capacitación en seguridad de la información, revisado y aprobado por la alta Dirección, con sus respectivos soportes.	Consolidación de Plan Institucional de Capacitación PIC.	No se tiene contemplado capacitaciones relacionadas son el tema de seguridad; sin embarga se tienen pensada para el plan del próximo año.
20	Documento que haga claridad sobre el proceso disciplinario en caso de incumplimiento de las políticas de seguridad de la información.	Acto administrativo 2130 de 2014, política de seguridad de la información.	
21	Inventario de activos de información clasificados, de la entidad, revisado y aprobado por la alta dirección.	Borrador en Excel Inventario Activos Datos- Información FPS-FNC v1.	Se cuenta en espera de aprobación del comité de desarrollo administrativo.
22	Inventario de áreas de procesamiento de información y telecomunicaciones.	Mapa de proceso.	
23	Diagrama de red de alto nivel o arquitectura de TI.		No se tiene.
24	Arquitectura de TI.		No se tiene.
25	Metodología de gestión de proyectos.	Procedimiento APAJUOAJPT16 Elaboración de estudio previo.	
26	Inventario de partes externas o terceros a los que se transfiere información de la entidad.	Proceso ESDESOPSFO11 Matriz de información primaria y secundaria.	
27	Formato de acuerdo de transferencia de información.		No se tiene para parte externa o terceros.
28	Inventario de proveedores que tengan acceso a los activos de información, indicando el servicio que prestan o bienes que venden.		No se tiene.
29	Reporte de eventos e incidentes de seguridad de la información del año 2015.		No se tiene.

Cuadro 1 (Continuación)

	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia	

N°	Datos e información a recolectar para la evaluación	Nombre del documento entregado	Observaciones
30	Plan de continuidad de la Entidad aprobado.	Guía para la formulación de planes de contingencia en el FPS ESDESDIGGS06 y ESDESDIGFO13 Formato Formulación Planes de contingencia.	Se encuentra fecha de actualización 2010.
31	Inventario de obligaciones legales, estatutarias, reglamentarias, normativas relacionadas con seguridad de la información.	APGDOSGEFO08 Nomograma institucional.	
32	Listado de auditorías relacionadas con seguridad de la información realizadas en la entidad.		No se tiene.
33	Procedimientos, manuales, guías, directrices, lineamientos, estándares, instructivos relacionados con seguridad de la información, el modelo de seguridad y privacidad de la información de MINTIC y Gobierno en Línea.	APGTS Gestión de TICs.	APGTSOPSPT01 - Publicación y actualización de información en medios electrónicos (Página web, intranet) APGTSOPSPT02 - Copias de seguridad de usuarios y servidores APGTSOPSPT03 - Soporte técnico a usuarios APGTSOPSPT04 - Asignación y rotación de equipos de computo APGTSOPSPT05 - Mantenimiento de servidor intranet APGTSOPSPT06 - Creación, modificación y eliminación de usuarios en el sistema APGTSOPSPT07 - Mantenimiento de servidor de aplicaciones y bases de datos.
34	Indicadores y métricas de seguridad de la información definidos.		Se definió un indicador en estos momentos se encuentra en revisión técnica.
35	Declaración de aplicabilidad	Borrador manual.	se tiene pero sin aprobación
36	Aceptación de los riesgos residuales por parte de los dueños de los riesgos.		No se tiene.

Cuadro 1. (Continuación)

	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia			
N°	**Datos e información a recolectar para la evaluación**	**Nombre del documento entregado**	**Observaciones**	
37	Alcance del MSPI.	Borrador en Word incluida en el Manual de Sistema de Gestión de Seguridad y Privacidad de la Información.		
38	Procedimientos de control documental del MSPI.		No se tiene.	
	Lista de información para aquellas entidades que hayan avanzado en la fase de IMPLEMENTACIÓN.			
39	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.		La entidad está en fase inicial.	
40	Avance en la ejecución del plan de tratamiento de riesgos.		La entidad está en fase inicial.	
41	Avance en la implementación de la estrategia de transición de IPv4 a Ipv6.		La entidad está en fase inicial.	
42	Indicadores de gestión del MSPI definidos, revisados y aprobados por la alta Dirección.		La entidad está en fase inicial.	
	Lista de información para aquellas entidades que hayan avanzado en la fase de EVALUACIÓN DE DESEMPEÑO.			
43	Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección.		La entidad está en fase inicial.	
44	Documento con el plan de auditorías internas y resultados, de acuerdo a lo establecido en el plan de auditorías, revisado y aprobado por la alta Dirección.		La entidad está en fase inicial.	
45	Resultado del seguimiento, evaluación y análisis del plan de tratamiento de riesgos, revisado y aprobado por la alta Dirección.		La entidad está en fase inicial.	
	Lista de información para aquellas entidades que hayan avanzado en la fase de MEJORA CONTINUA			
46	Documento con el plan de seguimiento, evaluación y análisis para el MSPI, revisado y aprobado por la alta Dirección.		La entidad está en fase inicial.	
47	Documento con el consolidado de las auditorías realizadas de acuerdo con el plan de auditorías, revisado y aprobado por la alta dirección y verifique como se asegura que los hallazgos, brechas, debilidades y oportunidades de mejora se subsanen, para asegurar la mejora continua.		La entidad está en fase inicial.	
	Porcentaje de cumplimiento del MSPI en los procesos de la entidad.	# Total de procesos.	# De procesos definidos en el alcance.	Total avance por procesos.
48	Con base al alcance definido en la política de seguridad y el total de procesos de la entidad, indicar los siguientes datos.	14	0	0%

Fuente: Instrumento de evaluación del MINTIC

Cuadro 2. Escala de evaluación

Tabla de Escala de Valoración de Controles ISO 27001:2013 ANEXO A		
Descripción	**Calificación**	**Criterio**
No Aplica	N/A	No aplica.
Inexistente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.
Fuente: Instrumento de evaluación del MINTIC		

Cuadro 3. Áreas Involucradas

	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (áreas Involucradas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia	
RESPONSABLE / AREA	**TEMA**	**FUNCIONARIO**
Control interno	Revisiones de seguridad de la información.	No se tiene funcionario.
	Revisión independiente de la seguridad de la información.	
	Cumplimiento con las políticas y normas de seguridad.	
	CUMPLIMIENTO	
	Auditoría Interna Plan	
	Auditoría Interna Ejecución y Subsanación de hallazgos y brechas.	
Gestión Talento Humano	Selección e investigación de antecedentes.	Dra. María Margarita Cárdenas (Oficina Jurídica) - María Yaneth Farfán (Gestión Talento Humano).
	Términos y condiciones del empleo.	
	GESTION DE SERVICIO SALUD	Dr. José Jaime Azar.
	Garantizar la prestación de los servicios de salud a todos los usuarios en términos de oportunidad, calidad y eficiencia y soportados en la normatividad aplicable.	
Subdirector de Prestaciones Sociales	GESTION DE PRESTACIONES ECONOMICAS	Dr. José Jaime Azar.
	Reconocer y ordenar el pago oportuno de las prestaciones económicas a que tengan derecho nuestros usuarios, conforme a las normas legales y convencionales y procedimientos establecidos.	
Secretaría General	ATENCIÓN AL CIUDADANO	Dr. Luis Alfredo Escobar.
	Brindar de forma oportuna y veraz la información solicitada por los usuarios, de tal manera que permita orientarlos para la realización de trámites y/o uso de los servicios que presta la entidad; como también controlar la adecuada atención de las quejas, reclamos y sugerencias presentadas por los usuarios y promover los mecanismos de participación ciudadana.	
Responsable de compras y adquisiciones	RELACIONES CON LOS PROVEEDORES	Administrativa (Dr. Luis Alberto Segura).
	Seguridad de la información en las relaciones con los proveedores.	
	Gestión de la prestación de servicios de proveedores.	

Cuadro 3. (Continuación)

	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (áreas Involucradas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia	
RESPONSABLE / AREA	**TEMA**	**FUNCIONARIO**
Responsable de la continuidad.	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	No se tiene funcionario establecido por la planta de Entidad pero dentro de la funciones del contratista que manera el tema de seguridad de la información se tiene establecido.
	Continuidad de la seguridad de la información.	
	Planificación de la continuidad de la seguridad de la información.	
	Implementación de la continuidad de la seguridad de la información.	
	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	
	Redundancias.	
	Disponibilidad de instalaciones de procesamiento de información.	
Responsable de la seguridad física.	SEGURIDAD FÍSICA Y DEL ENTORNO	No se tiene funcionario establecido por la planta de Entidad pero dentro de la funciones del contratista que manera el tema de seguridad de la información se tiene establecido.
	ÁREAS SEGURAS	
	Perímetro de seguridad física.	
	Áreas de despacho y carga.	
	Visita al Centro de Cómputo.	Gestión TICs - Dr. Mauricio Villaneda.
Secretaría General	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	Dr. Luis Alfredo Escobar.
	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	
Responsable de compras y adquisiciones	SEGURIDAD DE LOS RECURSOS HUMANOS	Administrativa (Dr. Luis Alberto Segura).
	Antes de asumir el empleo.	
	Durante la ejecución del empleo.	
Responsable de SI	Terminación y cambio de empleo.	Gestión TICs - Dr. Mauricio Villaneda - Roselys Silva.
	GESTIÓN DE ACTIVOS	
	CUMPLIMIENTO	
	Cumplimiento de requisitos legales y contractuales.	
	CONTROL DE ACCESO	
	CRIPTOGRAFÍA	
	SEGURIDAD FÍSICA Y DEL ENTORNO	
	SEGURIDAD DE LAS OPERACIONES	
	PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	
	Procedimientos de operación documentados.	
	Gestión de cambios.	
	Gestión de capacidad.	
	Separación de los ambientes de desarrollo, pruebas y operación.	
	PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS	
	COPIAS DE RESPALDO	

Cuadro 3. (Continuación)

	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (áreas involucradas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia	
RESPONSABLE / AREA	**TEMA**	**FUNCIONARIO**
Responsable de SI.	REGISTRO Y SEGUIMIENTO Registro de eventos. Protección de la información de registro. Registros del administrador y del operador. Sincronización de relojes. CONTROL DE SOFTWARE OPERACIONAL Instalación de software en sistemas operativos. GESTIÓN DE LA VULNERABILIDAD TÉCNICA Gestión de las vulnerabilidades técnicas. Restricciones sobre la instalación de software. CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN Controles sobre auditorías de sistemas de información. SEGURIDAD DE LAS COMUNICACIONES GESTIÓN DE LA SEGURIDAD DE LAS REDES TRANSFERENCIA DE INFORMACIÓN ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE DATOS DE PRUEBA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Alcance MSPI (Modelo de Seguridad y Privacidad de la Información). Identificación y valoración de riesgos. Tratamiento de riesgos de seguridad de la información. Toma de conciencia, educación y formación en la seguridad de la información. Planificación y control operacional Implementación del plan de tratamiento de riesgos. Indicadores de gestión del MSPI. Plan de seguimiento, evaluación y análisis del MSPI. Evaluación del plan de tratamiento de riesgos.	Gestión TICs - Dr. Mauricio Villaneda - Roselys Silva.

Cuadro 3. (Continuación)

	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (áreas involucradas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia	
RESPONSABLE / AREA	**TEMA**	**FUNCIONARIO**
Responsable de SI.	Plan de seguimiento, evaluación y análisis del MSPI.	Gestión TICs - Dr. Mauricio Villaneda - Roselys Silva.
	Tratamiento de temas de seguridad y privacidad de la información en los comités del modelo integrado de gestión, o en los comités directivos interdisciplinarios de la Entidad.	
	Con base en el inventario de activos de información clasificado, se establece la caracterización de cada uno de los sistemas de información.	
	La entidad conoce su papel dentro del estado Colombiano, identifica y comunica a las partes interesadas la infraestructura crítica.	
	Las prioridades relacionadas con la misión, objetivos y actividades de la Entidad son establecidas y comunicadas.	
	La gestión de riesgos tiene en cuenta los riesgos de Ciberseguridad.	
	Detección de actividades anómalas.	
	Respuesta a incidentes de Ciberseguridad, planes de recuperación y restauración.	
Responsable de TICs.	Teletrabajo.	Gestión TICs - Mauricio Villaneda y Dema Consuelo Fernández.
	Manejo de medios.	
	Derechos de propiedad intelectual.	
	CONTROL DE ACCESO	
	SEGURIDAD DE LAS OPERACIONES	
	PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	
	COPIAS DE RESPALDO	
	CONTROL DE SOFTWARE OPERACIONAL	
	CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN	
	SEGURIDAD DE LAS COMUNICACIONES	
	GESTIÓN DE LA SEGURIDAD DE LAS REDES	
	TRANSFERENCIA DE INFORMACIÓN	
	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	
	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	
	Plan y Estrategia de transición de IPv4 a IPv6.	

Cuadro 3. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (áreas involucradas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia	vive digital para la gente
RESPONSABLE / AREA	**TEMA**	**FUNCIONARIO**
Responsable de SI.	Implementación del plan de estrategia de transición de IPv4 a IPv6.	Gestión TICs - Dr. Mauricio Villaneda - Roselys Silva.
	Redundancias.	
Calidad.	Procedimientos de control documental del MSPI.	Oficina de Planeación - Dr. Mauricio Villaneda.
Fuente: Instrumento de evaluación del MINTIC		

Cuadro 4. Administrativa

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Administrativa) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN										
AD.1	**Responsable de SI**	**POLITICAS DE SEGURIDAD DE LA INFORMACIÓN**	**Orientación de la dirección para gestión de la seguridad de la información**	**A.5**	**Componente planificación y modelo de madurez nivel gestionado**				30	
AD.1.1	Responsable de SI	Documento de la política de seguridad y privacidad de la Información.	Se debe definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y comunicada a los empleados y a la partes externas pertinentes	A.5.1.1	Componente planificación y modelo de madurez inicial	Solicite la política de seguridad de la información de la entidad y evalúe: a) Si se definen los objetivos, alcance de la política. b) Si esta se encuentra alineada con la estrategia y objetivos de la entidad c) Si fue debidamente aprobada y socializada al interior de la entidad por la alta dirección Revise si la política: a)Define que es seguridad de la información b) La asignación de las responsabilidades generales y específicas para la gestión de la seguridad de la información, a roles definidos; c) Los procesos para manejar las desviaciones y las excepciones. Indague sobre los responsables designados formalmente por la dirección para desarrollar, actualizar y revisar las políticas. Verifique cada cuanto o bajo qué circunstancias se revisan y actualizan, verifique la última fecha de emisión de la política frente a la fecha actual y que cambios a sufrido, por lo menos debe haber una revisión anual. Para la calificación tenga en cuenta que: 1) Si se empiezan a definir las políticas de seguridad y privacidad de la información basada en el Modelo de Seguridad y Privacidad de la Información, están en 20. 2) Si se revisan y se aprueban las políticas de seguridad y privacidad de la información, están en 40. 3) Si se divulgan las políticas de seguridad y privacidad de la información, están en 60.	Acto administrativo 2130 de 2014, política de seguridad de la información Listado de eventos de las capacitaciones donde se socializo la política.	No se define que es seguridad de la información. No se tiene asignación de las responsabilidades generales y específicas para la gestión de la seguridad de la información, a roles definidos. No se tienen los procesos para manejar las desviaciones y excepciones.	40	Actualizar la política subsanando las brechas descritas.
AD.1.2	Responsable de SI	Revisión y evaluación.	Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.	A.5.1.2	Componente planificación			Se creó en la fecha: 27 de agosto de 2014, se tiene una actualización de fecha: 31 de agosto de 2016 sin embargo esta no ha sido aprobada.		Una vez actualizada la política, establecer cada cuanto se debe realizar revisión y actualización de la misma.

Cuadro 4. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Administrativa) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
RESPONSABILIDADES Y ORGANIZACIÓN SEGURIDAD INFORMACIÓN										
A2	**Responsable de SI**	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	**"Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización**	**A.6**					**26**	
AD.2.1	**Responsable de SI**	**Organización Interna**	**Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización**	**A.6.1**	Componente planificación y modelo de madurez inicial				52	
Responsable de SI	Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	A.6.1.1	Componente planificación.	Responsable de SI	Para revisarlo frente a la NIST verifique si 1) los roles y responsabilidades frente a la ciberseguridad han sido establecidos 2) los roles y responsabilidades de seguridad de la información han sido coordinados y alineados con los roles internos y las terceras partes externas 3) Los a) proveedores, b) clientes, c) socios, d) funcionarios, e) usuarios privilegiados, f) directores y gerentes (mandos sénior), g) personal de seguridad física, h) personal de seguridad de la información entienden sus roles y responsabilidades, i) Están claros los roles y responsabilidades para la detección de incidentes Solicite el acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o es que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección. Revise la estructura del SGSI: 1) ¿Tiene el SGSI suficiente apoyo de la alta dirección?, esto se ve reflejado en comités donde se discutan temas como la política de SI, los riesgos o incidentes. 2) ¿Están claramente definidos los roles y responsabilidades y asignados a personal con las competencias requeridas?, 3) Están identificadas los responsables y responsabilidades para la protección de los activos? (Una práctica común es nombrar un propietario para cada activo, quien entonces se convierte en el responsable de su protección) 4) ¿Están definidas las responsabilidades para la gestión del riesgo de SI y la aceptación de los riesgos residuales? 5) ¿Están definidos y documentados los niveles de autorización? 6) Se cuenta con un presupuesto formalmente asignado a las actividades del SGSI (por ejemplo campañas de sensibilización en seguridad de la información)	Borrador en Word Manual del Sistema de Gestión de Seguridad y Privacidad de la Información Acto administrativo 2129 de 2014 Borrador en Excel Inventario Activos Datos-Información FPS-FNC v1.	Dentro del borrador no se tienen los roles frente a la ciberseguridad establecidos, Teniendo en cuenta que el documento es un borrador hay roles que no se han socializado formalmente, no se tiene claridad en los roles y responsabilidades para la detección de incidentes. El acto administrativo define el comité como tal, sin embargo a la fecha, se tiene un comité que centraliza todo incluyendo los temas de seguridad de la información, actualmente se tiene un borrador con el inventario de activos y sus responsables pero no ha sido aprobado. No se encuentran definidas las responsabilidades para la gestión del riesgo de SI y la aceptación de riesgos residuales, tampoco están documentados los niveles de autorización, ni se cuenta con un presupuesto formalmente asignado a las actividades de SGSI, el que existe es el general y de allí salen recursos pero no.	20	Ajustar el borrador tanto del Manual de Sistema de Gestión de la Seguridad de la Información y el de inventario de Activos, subsanando las brechas encontradas.

Cuadro 4. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Administrativa) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
RESPONSABILIDADES Y ORGANIZACIÓN SEGURIDAD INFORMACIÓN										
A2	**Responsable de SI**	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	**"Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización**	**A.6**					26	
AD.2.1.2	Responsable de SI	Separación de deberes / tareas	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	A.6.1.2		Indague como evitan que una persona pueda acceder, modificar o usar activos sin autorización ni detección. La mejor práctica dicta que el inicio de un evento deber estar separado de su autorización. Al diseñar los controles se debería considerar la posibilidad de confabulación. Tenga en cuenta que Para las organizaciones pequeñas la separación de deberes puede ser difícil de lograr, en estos casos se deben considerar controles compensatorios como revisión periódica de, los rastros de auditoría y la supervisión de cargos superiores.	APGTSOPSPT06 Procedimiento creación, modificación y Eliminación de usuarios del sistema.		100	
AD.2.1.3	Responsable de SI	Contacto con las autoridades.	Las organizaciones deben tener procedimientos establecidos que especifiquen cuándo y a través de que autoridades se debe contactar a las autoridades (por ejemplo, las encargadas de hacer cumplir la ley, los organismos de reglamentación y las autoridades de supervisión), y cómo se debe reportar de una manera oportuna los incidentes de seguridad de la información identificados (por ejemplo, si se sospecha una violación de la ley).	A.6.1.3		Solicite los procedimientos establecidos que especifiquen cuándo y a través de que autoridades se debería contactar a las autoridades, verifique si de acuerdo a estos procedimientos se han reportado eventos o incidentes de SI de forma consistente.	APGDOSGEPT22 Procedimiento proceso disciplinario ordinario y APGDOSGEPT23 Procedimiento proceso disciplinario verbal.	Incluir cuando tenga que ver con un incidente de seguridad de la información.	40	.
AD.2.1.4	Responsable de SI	Contacto con grupos de interés especiales	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad. Por ejemplo a través de una membrecía	A.6.1.4		Pregunte sobre las membrecías en grupos o foros de interés especial en seguridad de la información en los que se encuentran inscritas las personas responsables de la SI.	Se le reporta incidentes de seguridad al Equipo de Respuesta a Incidentes de Seguridad Informática CSIRT.		100	
AD.2.1.5	Responsable de SI	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe integrar al(los) método(s) de gestión de proyectos de la organización, para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte de un proyecto. Esto se aplica generalmente a cualquier proyecto, independientemente de su naturaleza, por ejemplo, un proyecto para un proceso del negocio principal, TI, gestión de instalaciones y otros procesos de soporte.	A.6.1.5		Pregunte como la Entidad integra la seguridad de la información en el ciclo de vida de los proyectos para asegurar que para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto. Tenga en cuenta que esto no solamente aplica para proyectos de TI, por ejemplo puede aplicar en proyectos de traslado de activos de información, gestión de instalaciones, personal en outsourcing que soporta procesos de la organización. Las mejores prácticas sugieren: a) Que los objetivos de la seguridad de la información se incluyan en los objetivos del proyecto; b) Que la valoración de los riesgos de seguridad de la información se lleve a cabo en una etapa temprana del proyecto, para identificar los controles necesarios; c) Que la seguridad de la información sea parte de todas las fases de la metodología del proyecto aplicada.	No se tiene.	Dentro de los proyectos siempre hay una matriz de riesgos pero no enfocada en riesgos de seguridad.	0	Incluir los riesgos de seguridad dentro de la matriz de riesgo de los proyectos.

Cuadro 4. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Administrativa) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
RESPONSABILIDADES Y ORGANIZACIÓN SEGURIDAD INFORMACIÓN										
AD.2.2	Responsable de SI	**Dispositivos Móviles y Teletrabajo**	**Garantizar la seguridad del teletrabajo y uso de dispositivos móviles**	**A.6.2**					**26**	
AD.2.2.1	Responsable de SI	Política para dispositivos móviles	Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	A.6.2.1		Pregunte si la entidad asigna dispositivos móviles a sus funcionarios o permite que los dispositivos de estos ingresen a la entidad. Revise si existe una política y controles para su uso, que protejan la información almacenada o procesada en estos dispositivos y el acceso a servicios te TI desde los mismos. De acuerdo a las mejores prácticas esta política debe considerar, teniendo en cuenta el uso que se le dé al dispositivo, lo siguiente: a) el registro de los dispositivos móviles; b) los requisitos de la protección física; c) las restricciones para la instalación de software; d) los requisitos para las versiones de software de dispositivos móviles y para aplicar parches; e) la restricción de la conexión a servicios de información; f) los controles de acceso; g) técnicas criptográficas; h) protección contra software malicioso; i) des habilitación remota, borrado o cierre; j) copias de respaldo; k) uso de servicios y aplicaciones web. Cuando la política de dispositivos móviles permite el uso de dispositivos móviles de propiedad personal, la política y las medidas de seguridad relacionadas también deben considerar: a) la separación entre el uso privado y de la Entidad de los dispositivos, incluido el uso del software para apoyar esta separación y proteger los datos del negocio en un dispositivo privado; b) brindar acceso a la información de la Entidad solo cuando los usuarios hayan firmado un acuerdo de usuario final, en el que se reconocen sus deberes (protección física, actualización del software, etc.), desistir de la propiedad de los datos de la Entidad, permitir el borrado remoto de datos por parte de la organización en caso de robo o pérdida del dispositivo, o cuando ya no se posee autorización para usar el servicio.	No se tiene.	No se tiene.	0	Incluir una política de dispositivos móviles.

Cuadro 4. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Administrativa) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
RESPONSABILIDADES Y ORGANIZACIÓN SEGURIDAD INFORMACIÓN										
AD.2.2.2	Responsable de TICs	Teletrabajo	Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	A.6.2.2		Definición de teletrabajo: El teletrabajo hace referencia a todas las formas de trabajo por fuera de la oficina, incluidos los entornos de trabajo no tradicionales, a los que se denomina "trabajo a distancia", "lugar de trabajo flexible", "trabajo remoto" y ambientes de "trabajo virtual". Indague con la entidad si el personal o terceros pueden realizar actividades de teletrabajo, si la respuesta es positiva solicite la política que indica las condiciones y restricciones para el uso del teletrabajo. Las mejores prácticas consideran los siguientes controles: a) la seguridad física existente en el sitio del teletrabajo b) los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la que se tendrá acceso y que pasará a través del enlace de comunicación y la sensibilidad del sistema interno; c) el suministro de acceso al escritorio virtual, que impide el procesamiento y almacenamiento de información en equipo de propiedad privada; d) la amenaza de acceso no autorizado a información o a recursos, por parte de otras personas que usan el mismo equipo, por ejemplo, familia y amigos; e) el uso de redes domésticas y requisitos o restricciones sobre la configuración de servicios de red inalámbrica; e) acuerdos de licenciamiento de software de tal forma que las organizaciones puedan llegar a ser responsables por el licenciamiento de software de los clientes en estaciones de trabajo de propiedad de los empleados o de usuarios externos; f) requisitos de firewall y de protección contra software malicioso. Las directrices y acuerdos que se consideren deberían incluir: g) el suministro de equipo adecuado y de muebles de almacenamiento para las actividades de teletrabajo, cuando no se permite el uso del equipo de propiedad privada que no está bajo el control de la organización; h) una definición del trabajo permitido, las horas de trabajo, la clasificación de la información que se puede mantener, y los sistemas y servicios internos a los que el tele trabajador está autorizado a acceder; i) el suministro de equipos de comunicación adecuados, incluidos los métodos para asegurar el acceso remoto; j) la revocación de la autoridad y de los derechos de acceso, y la devolución de los equipos cuando las actividades del teletrabajo finalicen.	La entidad no maneja teletrabajo		0	

Cuadro 4. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (administrativa) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
SEGURIDAD DE LOS RECURSOS HUMANOS										
AD.3	**Responsable de SI/Gestión Humana/Líderes de los procesos**	**SEGURIDAD DE LOS RECURSOS HUMANOS**		**A.7**					31	
AD.3.1	**Responsable de SI**	**Antes de asumir el empleo**	**Asegurar que el personal y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que son considerados.**	**A.7.1**	**Modelo de Madurez Definido**				60	
AD.3.1.1	Gestión Humana	Selección e investigación de antecedentes	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	A.7.1.1		Revise el proceso de selección de los funcionarios y contratistas, verifique que se lleva a cabo una revisión de: a) Referencias satisfactorias b) Verificación de la de la hoja de vida del solicitante incluyendo certificaciones académicas y laborales; c) Confirmación de las calificaciones académicas y profesionales declaradas; d) Una verificación más detallada, como la de la información crediticia o de antecedentes penales. Cuando un individuo es contratado para un rol de seguridad de la información específico, las organizaciones deberían asegurar que el candidato tenga la competencia necesaria para desempeñar el rol de seguridad; e) sea confiable para desempeñar el rol, especialmente si es crítico para la organización. f) Cuando un trabajo, ya sea una asignación o una promoción, implique que la persona tenga acceso a las instalaciones de procesamiento de información, y en particular, si ahí se maneja información confidencial, por ejemplo, información financiera o información muy confidencial, la organización debería también considerar verificaciones adicionales más detalladas (por ejemplo estudio de seguridad, polígrafo, visita domiciliaria) g) También se debería asegurar un proceso de selección para contratistas. En estos casos, el acuerdo entre la organización y el contratista debería especificar las responsabilidades por la realización de la selección, y los procedimientos de notificación que es necesario seguir si la selección no se ha finalizado, o si los resultados son motivo de duda o inquietud. h) La información sobre todos los candidatos que se consideran para cargos dentro de la organización, se debería recolectar y manejar apropiadamente de acuerdo con la ley de protección de datos personales.	Procedimiento 60APAJUOAJPT09 Registro hojas de vida y contratos en el SIGEP-APGTHGTHPT07 Procedimiento proceso vinculación de personal de planta		100	

Cuadro 4. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Administrativa) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
SEGURIDAD DE LOS RECURSOS HUMANOS										
AD.3.1.2	Gestión Humana	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	A.7.1.2		Modelo contrato u orden de servicios.	Solo se cuenta con una cláusula de confidencialidad dentro de los diferentes tipos de contrato.	20	Incluir el tema de seguridad de la información dentro de los diferentes tipos de contrato.	Modelo contrato u orden de servicios.
AD.3.2	**Responsable de SI/Líderes de los procesos**	**Durante la ejecución del empleo**	**Asegurar que los funcionarios y contratistas tomen consciencia de sus responsabilidades sobre la seguridad de la información y las cumplan.**	**A.7.1.2**	**Modelo de Madurez Definido**			33		
AD.3.2.1	Responsable de SI	Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	A.7.2.1		De acuerdo a la NIST los contratistas deben estar coordinados y alineados con los roles y responsabilidades de seguridad de la información. Indague y solicite evidencia del como la dirección se asegura de que los empleados y contratistas: a) Estén debidamente informados sobre sus roles y responsabilidades de seguridad de la información, antes de que se les otorgue el acceso a información o sistemas de información confidenciales. b) Se les suministren las directrices que establecen las expectativas de seguridad de la información de sus roles dentro de la Entidad. c) Logren un nivel de toma de conciencia sobre seguridad de la información pertinente a sus roles y responsabilidades dentro de la organización y estén motivados para cumplir con las políticas. d) Tengan continuamente las habilidades y calificaciones apropiadas y reciban capacitación en forma regular. e) Cuenten con un canal para reporte anónimo de incumplimiento de las políticas o procedimientos de seguridad de la información (“denuncias internas”).	Se tiene una política de seguridad del información que todos los funcionarios y contratista deben cumplir además se establece dentro de los contratos que se debe cumplir con las políticas y lineamientos de la entidad.	Solo se cuenta con una cláusula de confidencialidad dentro de los diferentes tipos de contrato.	20	

Cuadro 4. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Administrativa) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
SEGURIDAD DE LOS RECURSOS HUMANOS										
AD.3.2.2	Responsable de SI/Líderes de los procesos	Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la Entidad, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	A.7.2.2	Componente planeación Modelo de Madurez Inicial	Entreviste a los líderes de los procesos y pregúnteles que saben sobre la seguridad de la información, cuáles son sus responsabilidades y como aplican la seguridad de la información en su diario trabajo. Pregunte como se asegura que los funcionarios, Directores, Gerentes y contratistas tomen conciencia en seguridad de la información, alineado con las responsabilidades, políticas y procedimientos existentes en la Entidad. Solicite el documento con el plan de comunicación, sensibilización y capacitación, con los respectivos soportes, revisado y aprobado por la alta Dirección. Verifique que se han tenido en cuenta buenas prácticas como: a) Desarrollar campañas, elaborar folletos y boletines. b) Los planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, están aprobados y documentados, por la alta Dirección c) Verifique que nuevos empleados y contratistas son objeto de sensibilización en SI. d) Indague cada cuanto o con qué criterios se actualizan los programas de toma de conciencia. e) Verifique que en las evidencias se puede establecer los asistentes al programa y el tema impartido. f) Incluir en los temas de toma de conciencia los procedimientos básicos de seguridad de la información (tales como el reporte de incidentes de seguridad de la información) y los controles de línea base (tales como la seguridad de las contraseñas, los controles del software malicioso, y los escritorios limpios). g) De acuerdo a NIST verifique que los funcionarios con roles privilegiados entienden sus responsabilidades y roles. **Para la calificación tenga en cuenta que:** Si Los funcionarios de la Entidad no tienen conciencia de la seguridad y privacidad de la información. Diseñar programas para la conciencia y comunicación, de las políticas de seguridad y privacidad de la información, **están en 20.** Si se observa en los funcionarios una conciencia de seguridad y privacidad de la información y los planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, deben estar aprobados y documentados, por la alta Dirección, **están en 40.** Si se han ejecutado los planes de toma de conciencia, comunicación y divulgación, de las políticas de seguridad y privacidad de la información, aprobados por la alta Dirección, **están en 60.**	Consolidación de Plan Institucional de Capacitación PIC	No se tiene contemplado capacitaciones relacionadas son el tema de seguridad; sin embargo se tienen pensadas para el plan del próximo año	20	

Cuadro 4. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Administrativa) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
SEGURIDAD DE LOS RECURSOS HUMANOS										
AD.3.2.3	Responsable de SI	Proceso disciplinario	Se debe contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	A.7.2.3		Pregunte cual es el proceso disciplinario que se sigue cuando se verifica que ha ocurrido una violación a la seguridad de la información, ¿quién y cómo se determina la sanción al infractor?.	Acto administrativo 2130 de 2014, política de seguridad de la información, APGDOSGEPT22 Procedimiento proceso disciplinario ordinario y APGDOSGEPT23 Procedimiento proceso disciplinario verbal	No está detallado el tema de seguridad de la información.	60	Detallar la parte de seguridad de la información
Responsable de SI	**Terminación y cambio de empleo**	**Proteger los intereses de la Entidad como parte del proceso de cambio o terminación de empleo.**	**A.7.3**	**Modelo de Madurez Definido**	**Responsable de SI**				0	
	Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.	A.7.3.1	Responsable de SI	Terminación o cambio de responsabilidades de empleo	Revisar los acuerdos de confidencialidad, verificando que deben acordar que después de terminada la relación laboral o contrato seguirán vigentes por un periodo de tiempo.	APGTHGTHPT06 Procedimiento entrega de cargos y APGTSOPSPT06 Procedimiento creación, modificación y eliminación de usuarios en el sistema	Ajustarlos al incumplimiento de los acuerdos de confidencialidad.	0	
GESTIÓN DE ACTIVOS										
AD.4	**Responsable de SI**	**GESTIÓN DE ACTIVOS**		**A.8**					24	
AD.4.1	**Responsable de SI**	**Responsabilidad de los activos**	**Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.**	**A.8.1**	**Modelo de Madurez Gestionado**				25	
AD.4.1.1	Responsable de SI	Inventario de activos	Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	A.8.1.1	Componente Planificación Modelo de madurez inicial	Solicite el inventario de activos de información, revisado y aprobado por la alta Dirección y revise: 1) Ultima vez que se actualizó 2) Que señale bajo algún criterio la importancia del activo 3) Que señale el propietario del activo Indague quien(es) el(los) encargado(s) de actualizar y revisar el inventario de activos y cada cuanto se realiza esta revisión. De acuerdo a NIST se deben considerar como activos el personal, dispositivos, sistemas e instalaciones físicas que permiten a la entidad cumplir con su misión y objetivos, dada su importancia y riesgos estratégicos. **Tenga en cuenta para la calificación:** 1) Si Se identifican en forma general los activos de información de la Entidad, están en 40. 2) Si se cuenta con un inventario de activos de información física y lógica de toda la entidad, documentado y firmado por la alta dirección, están en 60. 3) Si se revisa y monitorean periódicamente los activos de información de la entidad, están en 80.	Borrador en Excel Inventario Activos Datos- Información FPS-FNC v1 y APGTSOPSPT Inventario, clasificación y etiquetado de activos de información	Ambos documentos son borradores, por tanto no se encuentran aprobados.	40	

Cuadro 4. (Continuación)

TODOS POR UN NUEVO PAÍS MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Administrativa) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
GESTIÓN DE ACTIVOS										
AD.4.1.2	Responsable de SI	Propiedad de los activos	Los activos mantenidos en el inventario deben tener un propietario.	A.8.1.2		Solicite el procedimiento para asegurar la asignación oportuna de la propiedad de los activos. Tenga en cuenta que la propiedad se debería asignar cuando los activos se crean o cuando son entregados a la Entidad. De acuerdo a las mejores prácticas el propietario de los activos (individuo o entidad, que es responsable por el activo) tiene las siguientes responsabilidades: a) asegurarse de que los activos están inventariados; b) asegurarse de que los activos están clasificados y protegidos apropiadamente; c) definir y revisar periódicamente las restricciones y clasificaciones de acceso a activos importantes, teniendo en cuenta las políticas de control de acceso aplicables; d) asegurarse del manejo apropiado del activo cuando es eliminado o destruido.	Borrador en Excel Inventario Activos Datos- Información FPS-FNC v1.	Es un borrador	20	
AD.4.1.3	Responsable de SI	Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	A.8.1.3		Pregunte por la política, procedimiento, directriz o lineamiento que defina el uso aceptable de los activos, verifique que es conocida por los empleados y usuarios de partes externas que usan activos de la Entidad o tienen acceso a ellos.	No se tiene.		0	Pregunte por la política, procedimiento, directriz o lineamiento que defina el uso aceptable de los activos, verifique que es conocida por los empleados y usuarios de partes externas que usan activos de la Entidad o tienen acceso a ellos.

Cuadro 4. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Administrativa) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
SEGURIDAD DE LOS RECURSOS HUMANOS										
AD.4.2	**Responsable de SI**	**Clasificación de información**	**Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la Entidad.**	**A.8.2**					20	
AD.4.2.1	Responsable de SI	Clasificación de la información	La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	A.8.2.1	Modelo de Madurez Inicial	Solicite el procedimiento mediante el cual se clasifican los activos de información y evalué: 1) Que las convenciones y criterios de clasificación sean claros y estén documentados 2) Que se defina cada cuanto debe revisarse la clasificación de un activo 3) La clasificación debería valorarse analizando la confidencialidad, integridad y disponibilidad. Solicite muestras de inventarios de activos de información clasificados y evalué que se aplican las políticas y procedimientos de clasificación definidos. Evalué si los procesos seleccionados aplican de manera consistente estas políticas y procedimientos.	Borrador en Excel Inventario Activos Datos- Información FPS-FNC v1 y APGTSOPSPT Inventario, clasificación y etiquetado de activos de información.	Ambos son borrador y falta aprobación	20	Solicite el procedimiento mediante el cual se clasifican los activos de información y evalué: 1) Que las convenciones y criterios de clasificación sean claros y estén documentados 2) Que se defina cada cuanto debe revisarse la clasificación de un activo 3) La clasificación debería valorarse analizando la confidencialidad, integridad y disponibilidad. Solicite muestras de inventarios de activos de información clasificados y evalué que se aplican las políticas y procedimientos de clasificación definidos. Evalué si los procesos seleccionados aplican de manera consistente estas políticas y procedimientos.

Cuadro 4. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Administrativa) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
SEGURIDAD DE LOS RECURSOS HUMANOS										
AD.4.2.2	Responsable de SI	Etiquetado de la información		A.8.2.2		Solicite el procedimiento para el etiquetado de la información y evalúe: 1) Aplica a activos en formatos físicos y electrónicos (etiquetas físicas, metadatos) 2) Que refleje el esquema de clasificación establecido 3) Que las etiquetas se puedan reconocer fácilmente 4) Que los empleados y contratistas conocen el procedimiento de etiquetado Revise en una muestra de activos el correcto etiquetado	APGTSOPSPT Inventario, clasificación y etiquetado de activos de información.	El procedimiento no se está aplicando porque no está aprobado	20	Solicite el procedimiento para el etiquetado de la información y evalúe: 1) Aplica a activos en formatos físicos y electrónicos (etiquetas físicas, metadatos) 2) Que refleje el esquema de clasificación establecido 3) Que las etiquetas se puedan reconocer fácilmente 4) Que los empleados y contratistas conocen el procedimiento de etiquetado Revise en una muestra de activos el correcto etiquetado.
AD.4.2.3	Responsable de SI	Manejo de activos		A.8.2.3		Solicite los procedimientos para el manejo, procesamiento, almacenamiento y comunicación de información de conformidad con su clasificación. De acuerdo a las mejores prácticas evidencie si se han considerado los siguientes asuntos: a) Restricciones de acceso que soportan los requisitos de protección para cada nivel de clasificación; b) Registro formal de los receptores autorizados de los activos; c) Protección de copias de información temporal o permanente a un nivel coherente con la protección de la información original; d) Almacenamiento de los activos de TI de acuerdo con las especificaciones de los fabricantes; e) Marcado claro de todas las copias de medios para la atención del receptor autorizado. f) De acuerdo a NIST la información almacenada (at resto) y en tránsito debe ser protegida.	APGTSOPSPT Inventario, clasificación y etiquetado de activos de información.		20	

Cuadro 4. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Administrativa) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
SEGURIDAD DE LOS RECURSOS HUMANOS										
AD.4.3	**Responsable de TICs**	**Manejo de medios**	**Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de la información almacenada en los medios.**	**A.8.3**					27	
AD.4.3.1	Responsable de TICs	Gestión de medios removibles		A.8.3.1		Solicite las directrices, guías, lineamientos y procedimientos para la gestión de medios removibles, que consideren: a) Si ya no se requiere, el contenido de cualquier medio reusable que se vaya a retirar de la organización se debe remover de forma que no sea recuperable; b) cuando resulte necesario y práctico, se debe solicitar autorización para retirar los medios de la organización, y se debe llevar un registro de dichos retiros con el fin de mantener un rastro de auditoría; d) si la confidencialidad o integridad de los datos se consideran importantes, se deben usar técnicas criptográficas para proteger los datos que se encuentran en los medios removibles; f) se deben guardar varias copias de los datos valiosos en medios separados, para reducir aún más el riesgo de daño o pérdida casuales de los datos; h) sólo se deben habilitar unidades de medios removibles si hay una razón de valida asociada a los procesos la Entidad para hacerlo; i) En donde hay necesidad de usar medios removibles, se debería hacer seguimiento a la transferencia de información a estos medios (Por ejemplo DLP)	no se tiene		0	
AD.4.3.2	Responsable de TICs	Disposición de los medios		A.8.3.2		Solicite los procedimientos existentes para garantizar que los medios a desechar o donar, no contienen información confidencial que pueda ser consultada y copiada por personas no autorizadas. Verifique si se ha realizado esta actividad y si existen registros de la misma.	no se tiene		0	
AD.4.3.3	Responsable de TICs	Transferencia de medios físicos		A.8.3.3		Solicite las directrices definidas para la protección de medios que contienen información durante el transporte. Verifique de acuerdo a las mejores prácticas que se contemple: a) El uso de un transporte o servicios de mensajería confiables. b) Procedimientos para verificar la identificación de los servicios de mensajería. c) Indague y evidencie como es el embalaje el cual debe proteger el contenido contra cualquier daño físico que pudiera presentarse durante el tránsito, y de acuerdo con las especificaciones de los fabricantes, por ejemplo, protección contra cualquier factor ambiental que pueda reducir la eficacia de la restauración del medio, tal como exposición al calor, humedad o campos electromagnéticos; d) Solicite los registros que dejen evidencia del transporte donde se identifique el contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte, y el recibo en su destino.	Convenio interadministrativo con 472		80	el transporte, y el recibo en su destino.

Cuadro 4. (Continuación)

TODOS POR UN NUEVO PAÍS MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Administrativa) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO										
AD.5	**Responsable de la Continuidad**	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**		**A.17**					**10**	
AD.5.1	**Responsable de la Continuidad**	**Continuidad de la seguridad de la información**	**La continuidad de la seguridad de la información debe incluir en los sistemas de gestión de la continuidad del negocio de la Entidad.**	**A.17.1**					20	
AD.5.1.1	Responsable de la Continuidad	Planificación de la continuidad de la seguridad de la información		A.17.1.1	Modelo de Madurez Gestionado	Indagar si la Entidad cuenta con un BCP (Bussiness Continuity Plan) o DRP (Disaster Recovery Plan). Determine si aplica para procesos críticos solamente o se han incluido otros procesos o por lo menos se ha reconocido la necesidad de ampliarlo a otros procesos (para determinar el nivel de madurez) Evalúe si se ha incluido en estos planes y procedimientos los requisitos de seguridad de la información. Tenga en cuenta que en ausencia de una planificación formal de continuidad de negocio y recuperación de desastres, la dirección de seguridad de la información debería suponer que los requisitos de seguridad de la información siguen siendo los mismos en situaciones adversas, en comparación con las condiciones operacionales normales. Como alternativa, una organización puede llevar a cabo un análisis de impacto en el negocio de los aspectos de seguridad de la información, para determinar los requisitos de seguridad de la información aplicables a situaciones adversas. De acuerdo a la NIST también se deben tener planes de respuesta a incidentes y recuperación de incidentes. **Tenga en cuenta para la calificación:** 1) Si existen planes de continuidad del negocio que contemplen los procesos críticos de la Entidad que garanticen la continuidad de los mismos. Se documentan tan y protegen adecuadamente los planes de continuidad del negocio de la Entidad, este de estar documentado y firmado, por la alta Dirección**, están en 40.** 2) Si se reconoce la importancia de ampliar los planes de continuidad de del negocio a otros procesos, pero aún no se pueden incluir ni trabajar con ellos, **están en 60.**	Guía para la formulación de planes de contingencia en el FPSS ESDESDIGGS06 y ESDESDIGFO13 Formato formulación planes de contingencia	Se tiene que actualizar incluyendo el tema de seguridad de la información	60	

Cuadro 4. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Administrativa) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
SEGURIDAD DE LOS RECURSOS HUMANOS										
AD.5.1.1	Responsable de la Continuidad	Planificación de la continuidad de la seguridad de la información		A.17.1.1	Modelo de Madurez Gestionado	Indagar si la Entidad cuenta con un BCP (Bussiness Continuity Plan) o DRP (Disaster Recovery Plan). Determine si aplica para procesos críticos solamente o se han incluido otros procesos o por lo menos se ha reconocido la necesidad de ampliarlo a otros procesos (para determinar el nivel de madurez) Evalúe si se ha incluido en estos planes y procedimientos los requisitos de seguridad de la información. Tenga en cuenta que en ausencia de una planificación formal de continuidad de negocio y recuperación de desastres, la dirección de seguridad de la información debería suponer que los requisitos de seguridad de la información siguen siendo los mismos en situaciones adversas, en comparación con las condiciones operacionales normales. Como alternativa, una organización puede llevar a cabo un análisis de impacto en el negocio de los aspectos de seguridad de la información, para determinar los requisitos de seguridad de la información aplicables a situaciones adversas. De acuerdo a la NIST también se deben tener planes de respuesta a incidentes y recuperación de incidentes. **Tenga en cuenta para la calificación:** 1) Si existen planes de continuidad del negocio que contemplen los procesos críticos de la Entidad que garanticen la continuidad de los mismos. Se documentan tan y protegen adecuadamente los planes de continuidad del negocio de la Entidad, este de estar documentado y firmado, por la alta Dirección**, están en 40.** 2) Si se reconoce la importancia de ampliar los planes de continuidad de del negocio a otros procesos, pero aún no se pueden incluir ni trabajar con ellos, **están en 60.**	Guía para la formulación de planes de contingencia en el FPSS ESDESDIGGS06 y ESDESDIGFO13 Formato formulación planes de contingencia	Se tiene que actualizar incluyendo el tema de seguridad de la información	60	
AD.5.1.2	Responsable de la Continuidad	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa,	A.17.1.2	Modelo de Madurez Definido	Verifique si la entidad cuenta con a) Una estructura organizacional adecuada para prepararse, mitigar y responder a un evento contingente, usando personal con la autoridad, experiencia y competencia necesarias. b) Personal formalmente asignado de respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para manejar un incidente y mantener la seguridad de la información. c) Planes aprobados, procedimientos de respuesta y recuperación documentados, en los que se especifique en detalle como la organización gestionará un evento contingente y mantendrá su seguridad de la información en un límite predeterminado, con base en los objetivos de continuidad de seguridad de la información aprobados por la dirección. Revise si los controles de seguridad de la información que se han implementado continúan operando durante un evento contingente. Si los controles de seguridad no están en capacidad de seguir brindando seguridad a la información, se la Entidad debe establecer, implementar y mantener otros controles para mantener un nivel aceptable de seguridad de la información.	no se tiene		0	

Cuadro 4. (Continuación)

TODOS POR UN NUEVO PAÍS MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Administrativa) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
SEGURIDAD DE LOS RECURSOS HUMANOS										
AD.5.2.1	Responsable de la Continuidad	Disponibilidad de instalaciones de procesamiento de información		A.17.2.1		Verifique si la Entidad cuenta con arquitecturas redundantes, ya sea un centro de cómputo principal y otro alterno o componentes redundantes en el único centro de cómputo. Indague como se han definido las necesidades de los procesos para seleccionar que elementos deben ser redundantes. Solicite si aplica las pruebas aplicadas para asegurar que un componente redundante funciona de la forma prevista durante una emergencia o falla.	No se cuenta con arquitecturas redundantes		0	
CUMPLIMIENTO										
AD.6	**Responsable de SI/Responsable de TICs/Control Interno**	**CUMPLIMIENTO**		**A.18**					27,5	
AD.6.1	**Responsable de SI**	**Cumplimiento de requisitos legales y contractuales**	**Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.**	**A.18.1**		**De acuerdo a la NIST: Los requerimientos legales y regulatorios respecto de la Ciberseguridad, incluyendo la privacidad y las libertades y obligaciones civiles, son entendidos y gestionados.**			55	
AD.6.1.1	Responsable de SI	Identificación de la legislación aplicable y de los requisitos contractuales.		A.18.1.1	**Modelo de Madurez Gestionado Cuantitativamente**	Solicite la relación de requisitos legales, reglamentarios, estatutarios, que le aplican a la Entidad (Nomograma). Indague si existe un responsable de identificarlos y se definen los responsables para su cumplimiento.	APGDOSGEFO08 Nomograma institucional y APGDOSGEPT03 Procedimiento control de documentos externos- Nomograma institucional, control interno hace verificación de cumplimiento en las auditorias que realiza		100	
AD.6.1.2	Responsable de TICs	Derechos de propiedad intelectual.		A.18.1.2		Verificación cumplimiento normas de uso de software (matriz primaria y secundaria) Y res18812011 políticas de buen uso y manejo de los equipos de cómputo, los servicios institucionales de correo electrónico e internet, Se tiene un software de seguridad que ayuda a que no se instalen aplicaciones ilegales (PCSecure), se tiene el inventario de software instalado	Falta comparar inventario de software instalado con número de licencias adquiridas, no hay control para asegurar que no se exceda ningún número máximo de usuarios permitido dentro de la licencia.	60	Verificación cumplimiento normas de uso de software (matriz primaria y secundaria) Y res18812011 políticas de buen uso y manejo de los equipos de cómputo, los servicios institucionales de correo electrónico e internet, Se tiene un software de seguridad que ayuda a que no se instalen aplicaciones ilegales (PCSecure), se tiene el inventario de software instalado	

Cuadro 4. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Administrativa) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
CUMPLIMIENTO										
AD.6.1.3	Responsable de SI	Protección de registros.	Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales	A.18.1.3		Revise si la Entidad cuenta con tablas de retención documental que especifiquen los registros y el periodo por el cual se deberían retener, además del almacenamiento, manejo y destrucción. Posibles tipos de registros pueden ser registros contables, registros de bases de datos, logs de transacciones, logs de auditoría y procedimientos operacionales, los medios de almacenamiento permitidos pueden ser papel, microfichas, medios magnéticos, medios ópticos etc.	APGDOSGEPT05 Procedimiento transferencias documentales al archivo central, APGDOSGEPT15 Procedimiento elaboración y actualización de las tablas de retención documental	Revisar y actualizar en caso que se requiera	40	
AD.6.1.4	Responsable de SI	Protección de los datos y privacidad de la información relacionada con los datos personales.	Se deben asegurar la protección y privacidad de la información personal tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.	A.18.1.4		Indague sobre las disposiciones que ha definido la Entidad para cumplir con la legislación de privacidad de los datos personales, ley estatutaria 1581 de 2012 y decreto 1377 que reglamenta la ley de 2013. 1) Revise si existe una política para cumplir con la ley 2) Si están definidos los responsables 3) Si se tienen identificados los repositorios de datos personales 4) Si se ha solicitado consentimiento al titular para tratar los datos personales y se guarda registro de este hecho. 5) Si se adoptan las medidas técnicas necesarias para proteger las bases de datos donde reposan estos datos.	MANUAL DE POLÍTICAS DE TRATAMIENTO DE DATOS PERSONALES	Es un borrador	20	
AD.6.1.5	n/a	Reglamentación de controles criptográficos.		A.18.1.5		n/a	no se tiene		0	
AD.6.2	**Control interno**	**Revisiones de seguridad de la información**		**A.18.2**					0	
AD.6.2.1	Control interno	Revisión independiente de la seguridad de la información		A.18.2.1		Investigue la forma como se realizan revisiones independientes (por personas diferentes o no vinculadas a un proceso o área que se revisa), de la conveniencia, la adecuación y la eficacia continuas de la gestionar la seguridad de la información. Para esto solicite: 1) El plan de auditorías del año 2015 2) El resultado de las auditorías del año 2015 3) Las oportunidades de mejora o cambios en la seguridad de la información identificados.	no se tiene		0	
AD.6.2.2	Control interno	Cumplimiento con las políticas y normas de seguridad.	Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.	A.18.2.2		1) Verifique si los gerentes aseguran que todos los procedimientos de seguridad dentro de su área de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento de las políticas y estándares de seguridad. 2) Verifique la revisión periódica del cumplimiento del centro de cómputo con las políticas y normas de seguridad establecidas. 3) Verifique si los sistemas de información son revisados regularmente para asegurar el cumplimiento de las normas de seguridad de la información.	no se tiene		0	

Cuadro 4. (Continuación)

TODOS POR UN NUEVO PAÍS MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Administrativa) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
CUMPLIMIENTO										
	Responsable de SI	Revisión de cumplimiento técnico.	Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.	A.18.2.3		Verifique si se realizan evaluaciones de seguridad técnicas por o bajo la supervisión de personal autorizado, apoyado en herramientas automáticas o con revisiones manuales realizadas por especialistas. Solicite evidencia de las últimas pruebas realizadas, sus resultados y seguimiento para asegurar que las brechas de seguridad fueron solucionadas.	no se tiene		0	
RELACIONES CON LOS PROVEEDORES										
AD.7	**Responsable de compras y adquisiciones**	**RELACIONES CON LOS PROVEEDORES**		**A.15**					10	
AD.7.1	Responsable de compras y adquisiciones	Seguridad de la información en las relaciones con los proveedores	Asegurar la protección de los activos de la entidad que sean accesibles para los proveedores	A.15.1	Modelo de Madurez Definido	1) Solicite la política de seguridad de la información para las relaciones con los proveedores, que indique los requisitos de SI para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización, esta política debe reflejarse en los acuerdos con los proveedores que deben estar documentados. 2) Verifique en la muestra de proveedores con acceso a los activos de información (no necesariamente son proveedores de tecnología de la información, por ejemplo pueden ser proveedores que tengan por ejemplo un proceso de nómina en outsourcing), se hayan suscrito acuerdos (ANS) formales donde se establezcan y acuerden todos los requisitos de seguridad de la información pertinentes con cada proveedor. 3) Verifique para los proveedores si se tiene en cuenta los riesgos de SI asociados a la cadena de suministro, por ejemplo para los proveedores en la nube es muy común que se apoyen en otros proveedores para proporcionar las instalaciones y se deben manejar los riesgos asociados a este tercero con el cual la entidad no tiene una relación comercial directa. Solicite que le indiquen como identifican para cada proveedor su cadena de suministro y obtenga evidencia de este hecho.	Borrador en Word incluida en el Manual del Sistema de Gestión de la Seguridad y Privacidad de la información	Incluir en las políticas específicas el tema de relaciones con proveedores	0	
AD.7.2	Responsable de compras y adquisiciones	Gestión de la prestación de servicios de proveedores	Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores	A.15.2	Modelo de Madurez Definido	1) Indague y solicite evidencia en una muestra de proveedores seleccionada, como la entidad hace seguimiento, revisa y audita con regularidad de acuerdo a la política la prestación de servicios de los proveedores y el cumplimiento de los compromisos respecto a la seguridad de la información. 2) Indague y evidencie como se gestionan los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, los incidentes de seguridad de la información y la revaloración de los riesgos. 2)	Se tiene una herramienta para evaluar proveedores pero Sta. Relacionada con la prestación del servicio pero no respecto a la seguridad de la información.		20	

Cuadro 4. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Administrativa) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.1.1.2	Responsable de TICs	Acceso a redes y a servicios en red	Se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	A.9.1.2		Revisar la política relacionada con el uso de redes y de servicios de red y verificar que incluya: a) las redes y servicios de red a los que se permite el acceso; b) los procedimientos de autorización para determinar a quién se permite el acceso a qué redes y servicios de red; c) los controles y procedimientos de gestión para proteger el acceso a las conexiones de red y a los servicios de red; d) los medios usados para acceder a las redes y servicios de red (uso de VPN o redes inalámbricas); e) los requisitos de autenticación de usuarios para acceder a diversos servicios de red; f) el seguimiento del uso de servicios de red.	No se tiene implementado	0		
T.1.2.3	Responsable de SI	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	A.9.2.3		Revisar la asignación de derechos de acceso privilegiado a través de un proceso de autorización formal de acuerdo con la política de control de acceso pertinente. el proceso debe incluir los siguientes pasos: a) Identificar los derechos de acceso privilegiado asociados con cada sistema o proceso, (sistema operativo, sistema de gestión de bases de datos, y cada aplicación) y los usuarios a los que es necesario asignar; b) definir o establecer los derechos de acceso privilegiado a usuarios con base en la necesidad de uso y caso por caso, alineada con la política de control de acceso; c) mantener un proceso de autorización y un registro de todos los privilegios asignados. Sólo se debe suministrar derechos de acceso cuando el proceso de autorización esté completo; d) definir los requisitos para la expiración de los derechos de acceso privilegiado; e) establecer los derechos de acceso privilegiado a través de una identificación de usuario diferente de la usada para las actividades regulares del negocio. Las actividades regulares del negocio no se ejecutan desde una identificación privilegiada; f) tener las competencias de los usuarios con derechos de acceso privilegiado y su revisión periódica para verificar si están en línea con sus deberes; g) establecer y mantener procedimientos genéricos para evitar el uso no autorizado de identificaciones de usuario de administración genérica, de acuerdo con las capacidades de configuración del sistema; h) establecer la confidencialidad de la información de autenticación secreta, para las identificaciones de usuario de administración genérica, cuando se comparta (cambiar las contraseñas con frecuencia, y cuando un usuario privilegiado ha dejado el trabajo o cambia de trabajo, comunicarlas entre los usuarios privilegiados con los mecanismos apropiados).	Colocar las condiciones faltantes dentro de la política de seguridad de la información	0		
T.1.2.4	Responsable de SI	Gestión de información de autenticación secreta de usuarios	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	A.9.2.4		Revisar el proceso, que incluya: a) establecer la firma de una declaración para mantener confidencial la información de autenticación secreta personal, y mantener la información de autenticación secreta del grupo (cuando es compartida) únicamente dentro de los miembros del grupo; esta declaración firmada se puede incluir en los términos y condiciones del empleo para todos los que los usuarios ; b) estipular que todos los usuarios deben mantener su propia información de autenticación secreta, y se les suministra una autentificación secreta temporal segura, que se obligue a cambiar al usarla por primera vez; c) establecer procedimientos para verificar la identidad de un usuario antes de proporcionarle la nueva información de autenticación secreta de reemplazo o temporal; d) definir que la información de autenticación secreta temporal se suministra a los usuarios de una manera segura; y se evitar utilizar partes externas o de mensajes de correo electrónico no protegidos (texto claro); e) establecer que la información de autenticación secreta temporal es única para un individuo y no es fácil de adivinar; f) definir que los usuarios deben acusar recibo de la información de autenticación secreta; g) establecer que la información de autenticación secreta por defecto, del fabricante, se modifica después de la instalación de los sistemas o software.		0		

Cuadro 5. Técnicas

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Técnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.1.2.5	Responsable de SI	Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	A.9.2.5		Revisar los derechos de acceso que incluya: a) examinar los derechos de acceso de los usuarios periódicamente y después de cualquier cambio, promoción, cambio a un cargo a un nivel inferior, o terminación del empleo; b) establecer que los derechos de acceso de usuario se revisan y reasignan cuando pasan de un rol a otro dentro de la misma organización; c) definir las autorizaciones para los derechos de acceso privilegiado y revisar periódicamente; d) verificar las asignaciones de privilegios periódicamente, para asegurar que no se hayan obtenido privilegios no autorizados; e) revisar y registrar los cambios a las cuentas privilegiadas periódicamente.		0		
T.1.2.6	Responsable de SI	Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	A.9.2.6		Revisar los derechos de acceso a la información y a los activos asociados con instalaciones de procesamiento de información, antes de que el empleo termine o cambie, dependiendo de la evaluación de factores de riesgo que incluya: a) terminación o cambio lo inicia el empleado, el usuario de la parte externa o la dirección, y la razón de la terminación; b) revisar las responsabilidades actuales del empleado, el usuario de la parte externa o cualquier otro usuario; c) verificar el valor de los activos accesibles en la actualidad.		0		
T.1.3	**Responsable de SI**	**RESPONSABILIDADES DE LOS USUARIOS**	**Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.**	**A.9.3**	Modelo de madurez definido	**No se tiene implementado**		**0**		
T.1.3.1	Responsable de SI	Uso de información de autenticación secreta	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	A.9.3.1		Revisar si el proceso de notificación a usuarios incluye: a) Mantener la confidencialidad de la información de autenticación secreta, asegurándose de que no sea divulgada a ninguna otra parte, incluidas las personas con autoridad; b) evitar llevar un registro (en papel, en un archivo de software o en un dispositivo portátil) de autenticación secreta, a menos que se pueda almacenar en forma segura y que el método de almacenamiento haya sido aprobado (una bóveda para contraseñas); c) cambiar la información de autenticación secreta siempre que haya cualquier indicio de que se pueda comprometer la información; d) definir que cuando se usa contraseñas como información de autenticación secreta, se debe seleccionar contraseñas seguras con una longitud mínima suficiente que: 1) sean fáciles de recordar; 2) no estén basadas en algo que otra persona pueda adivinar fácilmente u obtener usando información relacionada con la persona, (nombres, números de teléfono y fechas de nacimiento, etc.); 3) no sean vulnerables a ataques de diccionario (es decir, no contienen palabras incluidas en los diccionarios); 4) estén libres de caracteres completamente numéricos o alfabéticos idénticos consecutivos; 5) si son temporales, cambiarlos la primera vez que se ingrese; e) no compartir información de autenticación secreta del usuario individual; f) establecer una protección apropiada de contraseñas cuando se usan éstas como información de autenticación secreta en procedimientos de ingreso automatizados, y estén almacenadas; g) no usar la misma información de autenticación secreta para propósitos de negocio y otros diferentes de estos.		0		

Cuadro 5. (Continuación)

			Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Técnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia							
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.1.4.3	Responsable de TICs	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	A.9.4.3		Revisar el sistema de gestión de contraseñas que incluya: a) cumplir el uso de identificaciones y contraseñas de usuarios individuales para mantener la rendición de cuentas; b) permitir que los usuarios seleccionen y cambien sus propias contraseñas e incluyan un procedimiento de confirmación para permitir los errores de entrada; c) Exigir por que se escojan contraseñas de calidad; d) Forzar a los usuarios cambiar sus contraseñas cuando ingresan por primera vez; e) Exigir por que se cambien las contraseñas en forma regular, según sea necesario: f) llevar un registro de las contraseñas usadas previamente, e impedir su reusó; g) no visualizar contraseñas en la pantalla cuando se está ingresando; h) almacenar los archivos de las contraseñas separadamente de los datos del sistema de aplicaciones; i) almacenar y transmitir las contraseñas en forma protegida.	Se menciona el tema de contraseñas pero muy a groso modo	0		
T.1.4.4	Responsable de TICs	Uso de programas utilitarios privilegiados	Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.	A.9.4.4		Revisar las directrices para el uso de programas utilitarios con la capacidad de anular los controles de sistemas y de aplicaciones, que incluyan. a) utilizar procedimientos de identificación, autenticación y autorización para los programas utilitarios; b) separar los programas utilitarios del software de aplicaciones; c) limitar el uso de programas utilitarios al número mínimo práctico de usuarios confiables y autorizados; d) autorizar el uso adhoc de programas utilitarios; e) limitar la disponibilidad de los programas utilitarios; f) registrar el uso de los programas utilitarios; g) definir y documentar los niveles de autorización para los programas utilitarios; h) retirar o deshabilitar todos los programas utilitarios innecesarios; i) No poner a disposición los programas utilitarios a los usuarios que tengan acceso a aplicaciones en sistemas en donde se requiera la separación de deberes.		0		
T.1.4.5	Responsable de TICs	Control de acceso a códigos fuente de programas	Se debe restringir el acceso a los códigos fuente de los programas.	A.9.4.5		Revisar el procedimiento para la gestión de códigos fuente de los programas, que incluya: a) definir en donde sea posible, las librerías de fuentes de programas no se deben mantener en los sistemas operativos; b) gestionar los códigos fuente de los programas y las librerías de las fuentes de los programas se debería hacer de acuerdo con procedimientos establecidos; c) establecer que el personal de soporte deben tener acceso restringido a las librerías de las fuentes de los programas; d) definir que la actualización de las librerías de fuentes de programas y elementos asociados, y la entrega de fuentes de programas a los programadores sólo se deben hacer una vez que se haya recibido autorización apropiada; e) establecer que los listados de programas se deben mantener en un entorno seguro; f) conservar un registro de auditoría de todos los accesos a la librerías de fuentes de programas; g) mantener y copiar las bibliotecas de fuentes de programas a través de procedimientos estrictos de control de cambios.		0		
T.2	**Responsable de SI**	**CRIPTOGRAFÍA**	**Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización Garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles**	**A.10**				0		

Cuadro 5. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (técnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.2.1	**Responsable de SI**	**CONTROLES CRIPTOGRÁFICOS**	**Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.**	**A.10.1**	Modelo de madurez gestionado cuantitativamente			0		
T.2.1.1	Responsable de SI	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	A.10.1.1		Revisar la política sobre el uso de la criptográfica, que incluya: a) establecer el enfoque de la dirección con relación al uso de controles criptográficos en toda la organización, incluyendo los principios generales bajo los cuales se deben proteger la información del negocio; b) realizar una valoración de riesgos, que identifique el nivel de protección requerida, teniendo en cuenta el tipo, fortaleza y calidad del algoritmo de encriptación requerido. c) utilizar la encriptación para la protección de información transportada por dispositivos de encriptación móviles o removibles, o a través de líneas de comunicación; d) gestionar las llaves y los métodos para la protección de llaves criptográficas y la recuperación de información encriptada, en el caso de llaves perdidas, llaves cuya seguridad está comprometida, o que están dañadas; e) establecer roles y responsabilidades, quién es responsable por: 1) la implementación de la política. 2) la gestión de llaves, incluida la generación de llaves; f) establecer las normas que se van a adoptar para la implementación efectiva en toda la organización (procesos del negocio); g) definir el impacto de usar información encriptada en los controles que dependen de la inspección del contenido.		0		
T.2.1.2	Responsable de SI	Gestión de llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.	A.10.1.2		Revisar el sistema de gestión de llaves que debe estar basado en un grupo establecido de normas, procedimientos y métodos seguros para: a) generar llaves para diferentes sistemas criptográficos y diferentes aplicaciones; b) generar y obtener certificados de llaves públicas; c) distribuir llaves a las entidades previstas, incluyendo la forma de recibir y activar las llaves; d) almacenar las llaves, incluyendo la forma en que los usuarios autorizados obtienen acceso a ellas; e) cambiar o actualizar las llaves, incluyendo las reglas sobre cuándo se deben cambiar y cómo hacerlo; f) dar tratamiento a las llaves cuya seguridad está comprometida; g) revocar las llaves, incluyendo la forma de retirarlas o desactivarlas, cuando la seguridad de las llaves ha estado comprometida, o cuando un usuario deja la organización; h) recuperar las llaves que estén pérdidas o dañadas; i) hacer copias de respaldo de las llaves o archivarlas; j) destruir las llaves; k) registrar y auditar las actividades relacionadas con gestión de llaves.		0		
T.3	**Responsable de la seguridad física/Responsable de SI/Líderes de los procesos**	**SEGURIDAD FÍSICA Y DEL ENTORNO**		**A.11**				0		
T.3.1	**Responsable de la seguridad física**	**ÁREAS SEGURAS**	**Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.**	**A.11.1**	Modelo de madurez definido	**Se cuenta con control de entrada en recepción que garantiza que solo el personal autorizado dispone de permiso de acceso, se tiene controles disuasivo dentro de las oficinas, salas e instalaciones de la entidad, como cámaras que permiten mitigar el acceso no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la entidad**		**0**		

Cuadro 5. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Técnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.3.1.1	Responsable de la seguridad física	Perímetro de seguridad física	Se debe definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.	A.11.1.1		Revisar las directrices relacionadas con los perímetros de seguridad física: a) definir los perímetros de seguridad, y el emplazamiento y fortaleza de cada uno de los perímetros deben depender de los requisitos de seguridad de los activos dentro del perímetro y de los resultados de una valoración de riesgos; b) establecer los perímetros de una edificación o sitio que contenga instalaciones de procesamiento de la información debe ser físicamente seguros; el techo exterior, las paredes y el material de los pisos del sitio deben ser de construcción sólida, y todas las paredes externas deben estar protegidas adecuadamente contra acceso no autorizado con mecanismos de control (barras, alarmas, cerraduras); las puertas y ventanas deben estar cerradas con llave cuando no hay supervisión, y se debe considerar protección externa para ventanas, particularmente al nivel del suelo; c) definir un área de recepción con vigilancia u otro medio para controlar el acceso físico al sitio o edificación; el acceso a los sitios y edificaciones debe estar restringido únicamente para personal autorizado; d) establecer cuando sea aplicable y construir barreras físicas para impedir el acceso físico no autorizado y la contaminación ambiental; e) establecer que todas las puertas contra incendio en un perímetro de seguridad deben tener alarmas, estar monitoreadas y probadas junto con las paredes, para establecer el nivel requerido de resistencia de acuerdo con normas regionales, nacionales e internacionales adecuadas; deben funcionar de manera segura de acuerdo al código local de incendios; f) instalar sistemas adecuados para detección de intrusos de acuerdo con normas nacionales, regionales o internacionales y se deben probar regularmente para abarcar todas las puertas externas y ventanas accesibles; las áreas no ocupadas deben tener alarmas en todo momento; también deben abarcar otras áreas, tales como las salas de computo o las salas de comunicaciones; g) establecer que las instalaciones de procesamiento de información gestionadas por la organización deben estar separadas físicamente de las gestionadas por partes externas.	se cuenta con un área de recepción con vigilancia u otro medio para controlar el acceso físico al sitio o edificación; el acceso a los sitios y edificaciones debe estar restringido únicamente para personal autorizado;	las otras especificaciones no se manejan	0	

Cuadro 5. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Técnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.3.1.3	Líderes de los procesos	Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	A.11.1.3		Revisar las siguientes directrices relacionadas con la seguridad a oficinas, recintos e instalaciones: a) establecer que las instalaciones clave deben estar ubicadas de manera que se impida el acceso del público; b) definir donde sea aplicable, las edificaciones deben ser discretas y dar un indicio mínimo de su propósito, sin señales obvias externas o internas, que identifiquen la presencia de actividades de procesamiento de información; c) establecer que las instalaciones deben estar configuradas para evitar que las actividades o información confidenciales sean visibles y audibles desde el exterior. El blindaje electromagnético también se debe ser el apropiado; d) definir los directorios y guías telefónicas internas que identifican los lugares de las instalaciones de procesamiento de información confidencial no deben ser accesibles a ninguna persona no autorizada.	No se tiene implementado		0	
T.3.1.4	Responsable de SI	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	A.11.1.4		De acuerdo a la NIST deben identificarse los elementos de resiliencia para soportar la entrega de los servicios críticos de la entidad.	Se tiene un plan de emergencia pero se encuentra desactualizado		0	
T.3.1.5	Responsable de SI	Trabajo en áreas seguras	Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.	A.11.1.5	Componente planeación	Revisar trabajo en área segura y las siguientes directrices: a) establecer que el personal solo debe conocer de la existencia de un área segura o de actividades dentro de un área segura, con base en lo que necesita conocer; b) definir que el trabajo no supervisado en áreas seguras se debe evitar tanto por razones de seguridad como para evitar oportunidades para actividades malintencionadas; c) establecer que las áreas seguras vacías deben estar cerradas con llave y se revisan periódicamente; d) no se permite el ingreso y uso de equipo fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, a menos que se cuente con autorización para ello.	No se tiene implementado		0	
T.3.1.6	Responsable de la seguridad física	Áreas de despacho y carga	Se debe controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	A.11.1.6		Revisar las siguientes directrices: a) establecer que el acceso al área de despacho y de carga desde el exterior de la edificación se debería restringir al personal identificado y autorizado; b) definir que el área de despacho y carga se debe diseñar de manera que los suministros se puedan cargar y descargar sin que el personal de despacho tenga acceso a otras partes de la edificación; c) establecer que las puertas externas de un área de despacho y carga se aseguran cuando las puertas internas están abiertas; d) definir que el material que ingresa se inspecciona y examina para determinar la presencia de explosivos, químicos u otros materiales peligrosos, antes de que se retiren del área de despacho y carga; e) establecer que el material que ingresa se registra de acuerdo con los procedimientos de gestión de activos al entrar al sitio; f) definir que los despachos entrantes y salientes se están separados físicamente, en donde sea posible; g) establecer que el material entrante se inspecciona para determinar evidencia de manipulación durante el viaje. Si se descubre esta manipulación, se debería reportar de inmediato al personal de seguridad.	No se tiene implementado		0	

Cuadro 5. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Técnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.3.2	**Responsable de SI**	**EQUIPOS**	**Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.**	**A.11.2**			Se tiene un control pero no se está ejecutando		0	
T.3.2.1	Responsable de SI	Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	A.11.2.1		Revisar las siguientes directrices para proteger los equipos: a) establecer que los equipos están ubicados de manera que se minimice el acceso innecesario a las áreas de trabajo; b) definir que las instalaciones de procesamiento de la información que manejan datos sensibles están ubicadas cuidadosamente para reducir el riesgo de que personas no autorizadas puedan ver la información durante su uso; c) establecer que las instalaciones de almacenamiento se aseguran para evitar el acceso no autorizado; d) definir que los elementos que requieren protección especial se salvaguardan para reducir el nivel general de protección requerida; e) establecer los controles para minimizar el riesgo de amenazas físicas y ambientales, (robo, incendio, explosivos, humo, agua (o falla en el suministro de agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo); f) establecer directrices acerca de comer, consumir líquidos y fumar en cercanías de las instalaciones de procesamiento de información; g) hacer seguimiento de las condiciones ambientales tales como temperatura y humedad, para determinar las condiciones que puedan afectar adversamente las instalaciones de procesamiento de información; h) proteger contra descargas eléctricas atmosféricas se debe aplicar a todas las edificaciones y se deben colocar filtros a todas las líneas de comunicaciones y de potencia entrantes, para la protección contra dichas descargas; i) considerar el uso de métodos de protección especial, tales como membranas para teclados, para equipos en ambientes industriales; j) proteger los equipos para procesamiento de información confidencial para minimizar el riesgo de fuga de información debido a emanaciones electromagnéticas.	Se tiene un centro de cómputo donde almacenan los equipos que procesan la información de la entidad esta cuenta los controles para minimizar el riesgo de amenazas físicas y ambientales, (robo, incendio, explosivos, humo, agua (o falla en el suministro de agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo); h) proteger contra descargas eléctricas atmosféricas se debe aplicar a todas las edificaciones y se deben colocar filtros a todas las líneas de comunicaciones y de potencia entrantes, para la protección contra dichas descargas, se tiene un director que no se debe definir, consumir líquidos y fumar en cercanías de las instalaciones de procesamiento de información	colocar las condiciones faltantes tales como a) establecer que los equipos están ubicados de manera que se minimice el acceso innecesario a las áreas de trabajo; b) definir que las instalaciones de procesamiento de la información que manejan datos sensibles están ubicadas cuidadosamente para reducir el riesgo de que personas no autorizadas puedan ver la información durante su uso; c) establecer que las instalaciones de almacenamiento se aseguran para evitar el acceso no autorizado; d) definir que los elementos que requieren protección especial se salvaguardan para reducir el nivel general de protección requerida; g) hacer seguimiento de las condiciones ambientales tales como temperatura y humedad, para determinar las condiciones que puedan afectar adversamente las instalaciones de procesamiento de información; i) considerar el uso de métodos de protección especial, tales como membranas para teclados, para equipos en ambientes industriales; j) proteger los equipos para procesamiento de información confidencial para minimizar el riesgo de fuga de información debido a emanaciones electromagnética	0	

Cuadro 5. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Técnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.3.2.2	Responsable de TICs	Servicios de suministro	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	A.11.2.2		Revisar los servicios de suministro (electricidad, telecomunicaciones, suministro de agua, gas, alcantarillado, ventilación y aire acondicionado) para que cumplan: a) cumplir con las especificaciones de los fabricantes de equipos y con los requisitos legales locales; b) evaluar regularmente en cuanto a su capacidad para estar al ritmo del crecimiento e interacciones del negocio con otros servicios de soporte; c) inspeccionar y probar regularmente para asegurar su funcionamiento apropiado; d) si es necesario, contar con alarmas para detectar mal funcionamiento; e) si es necesario, tener múltiples alimentaciones con diverso enrutador físico.	No se tiene implementado		0	
T.3.2.3	Responsable de TICs	Seguridad del cableado	El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debe estar protegido contra interceptación, interferencia o daño.	A.11.2.3		Revisar las siguientes directrices para seguridad del cableado: a) establecer que las líneas de potencia y de telecomunicaciones que entran a instalaciones de procesamiento de información deben ser subterráneas en donde sea posible, o deben contar con una protección alternativa adecuada; b) establecer que los cables de potencia están separados de los cables de comunicaciones para evitar interferencia; c) definir para sistemas sensibles o críticos los controles adicionales que se deben considerar incluyen: 1) la instalación de conduit apantallado y recintos o cajas con llave en los puntos de inspección y de terminación; 2) el uso de blindaje electromagnético para proteger los cables; 3) el inicio de barridos técnicos e inspecciones físicas de dispositivos no autorizados que se conectan a los cables	No se tiene implementado		0	
T.3.2.4	Responsable de TICs	Mantenimiento de equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	A.11.2.4		Revisar las siguientes directrices para mantenimiento de equipos: a) mantener los equipos de acuerdo con los intervalos y especificaciones de servicio recomendados por el proveedor; b) establecer que solo el personal de mantenimiento autorizado debería llevar a cabo las reparaciones y el servicio a los equipos; c) llevar registros de todas las fallas reales o sospechadas, y de todo el mantenimiento preventivo y correctivo; d) implementar los controles apropiados cuando el equipo está programado para mantenimiento, teniendo en cuenta si éste lo lleva a cabo el personal en el sitio o personal externo a la organización; en donde sea necesario, la información confidencial se debe borrar del equipo, o el personal de mantenimiento debería retirarse (cleared) lo suficientemente de la información; e) cumplir todos los requisitos de mantenimiento impuestos por las políticas de seguros; f) establecer que antes de volver a poner el equipo en operación después de mantenimiento, se debería inspeccionar para asegurarse de que no ha sido alterado y que su funcionamiento es adecuado.	Se tiene estos procedimientos APGTSOPSPT07 - Mantenimiento de servidor de aplicaciones y base de datos - APGTSOPSPT05 - Mantenimiento de servidor de intranet y a parte se establece un contrato de mantenimiento semestralmente	No se tiene registros de todas las fallas reales o sospechadas, y de todo el mantenimiento preventivo y correctivo, controles apropiados cuando el equipo está programado para mantenimiento, teniendo en cuenta si éste lo lleva a cabo el personal en el sitio o personal externo a la organización; en donde sea necesario, la información confidencial se debe borrar del equipo, o el personal de mantenimiento debería retirarse (cleared) lo suficientemente de la información;	0	

Cuadro 5. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Tecnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.3.2.5	Responsable de TICs	Retiro de activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	A.11.2.5		Revisar las siguientes directrices para el retiro de activos: a) identificar a los empleados y usuarios de partes externas que tienen autoridad para permitir el retiro de activos del sitio; b) establecer los límites de tiempo para el retiro de activos y verificar que se cumplen las devoluciones; c) definir cuando sea necesario y apropiado, registrar los activos se retiran del sitio y cuando se hace su devolución; d) documentar la identidad, el rol y la filiación de cualquiera que maneje o use activos, y devolver esta documentación con el equipo, la información y el software. Información adicional	Se tiene establecido el procedimiento APGSAGADPT03 Administración cuentas personales bienes devolutivos, pero no cuenta con las directrices para el retiro de activos.		0	
T.3.2.6	Responsable de SI	Seguridad de equipos y activos fuera de las instalaciones	Se debe aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	A.11.2.6		De acuerdo a la NIST se deben catalogar los sistemas de información externos. Revisar las siguientes directrices para proteger los equipos fuera de las instalaciones: a) establecer que los equipos y medios retirados de las instalaciones no se deben dejar sin vigilancia en lugares públicos; b) seguir en todo momento las instrucciones del fabricante para proteger los equipos, (contra exposición a campos electromagnéticos fuertes); c) controlar los lugares fuera de las instalaciones, tales como trabajo en la casa, teletrabajo y sitios temporales se deben determinar mediante una valoración de riesgos y se deben aplicar los controles adecuados según sean apropiados, (gabinetes de archivo con llave, política de escritorio limpio, controles de acceso para computadores y comunicación segura con la oficina); d) establecer que cuando el equipo que se encuentra afuera de las instalaciones es transferido entre diferentes individuos y partes externas, llevar un registro que defina la cadena de custodia para el equipo, que incluya al menos los nombres y las organizaciones de los responsables del equipo.	No se tiene implementado		0	
T.3.2.7	Responsable de TICs	Disposición segura o reutilización de equipos	Se debe verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reusó.	A.11.2.7		Revisar las siguientes directrices del proceso de borrado de discos y de encriptación del disco (para evitar la divulgación de la información confidencial cuando se dispone del equipo o se le da un destino diferente, siempre y cuando): a) establecer que el proceso de encriptación sea suficientemente fuerte y abarque todo el disco (incluido el espacio perdido, archivos temporales de intercambio, etc.); b) definir que las llaves de encriptación sean lo suficientemente largas para resistir ataques de fuerza bruta; c) establecer que las llaves de encriptación se mantengan confidenciales.	No se tiene implementado		0	
T.3.2.8	Responsable de SI	Equipos de usuario desatendidos	Los usuarios deben asegurarse de que a los equipos desatendidos se les dé protección apropiada.	A.11.2.8		Revisar que el procedimiento equipos de usuarios desatendidos incluya: a) establecer que se cierren las sesiones activas cuando hayan terminado, a menos que se puedan asegurar mediante un mecanismo de bloqueo apropiado (un protector de pantalla protegido con contraseña); b) establecer que es obligatorio salir de las aplicaciones o servicios de red cuando ya no los necesiten; c) asegurar que los computadores o dispositivos móviles contra uso no autorizado mediante el bloqueo de teclas o un control equivalente (acceso con contraseña, cuando no están en uso).	Se cuenta establecido en procedimiento de aplicaciones que cuenta pero no se hace seguimiento del cumplimiento		0	

Cuadro 5. (Continuación)

	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Técnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia									
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.3.2.9	Responsable de SI	Política de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	A.11.2.9		Revisar las siguientes directrices para escritorio limpio: a) establecer que la información sensible o crítica del negocio, (sobre papel o en un medio de almacenamiento electrónico), se guarda bajo llave (idealmente, en una caja fuerte o en un gabinete u otro mueble de seguridad) cuando no se requiera, especialmente cuando la oficina esté desocupada. b) definir un procedimiento para la gestión de equipos desatendidos; los computadores y terminales deben estar fuera del sistema y estar protegidos con un sistema de bloqueo de la pantalla y el teclado, controlado por una contraseña, token o mecanismo similar de autenticación de usuario, y deben estar protegidos por bloqueo de teclas u otros controles, cuando no están en uso; c) evitar el uso no autorizado de fotocopiadoras y otra tecnología de reproducción (escáneres, cámaras digitales); d) establecer que los medios que contienen información sensible o clasificada se deben retirar de las impresoras inmediatamente.	No se tiene implementado		0	
T.4	**Responsable de TICs/Responsable de SI**	**SEGURIDAD DE LAS OPERACIONES**		**A.12**					6	
T.4.1	**Responsable de TICs**	**PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES**	**Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.**	**A.12.1**	Modelo de madurez definido		Se tiene procedimiento de operación, pero no se maneja Gestión de cambios, Gestión de capacidades y Separación de entornos de desarrollo, prueba y producción:		**0**	

Cuadro 5. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Técnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.4.1.1	**Responsable de TICs**	Procedimientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.	A.12.1.1		Revisar los procedimientos de operación con instrucciones operacionales, que incluyen: a) instalar y configurar sistemas; b) establecer el procesamiento y manejo de información, tanto automático como manual; c) establecer la gestión de las copias de respaldo; d) definir los requisitos de programación, incluidas las interdependencias con otros sistemas, los tiempos de finalización del primer y último trabajos; e) establecer las instrucciones para manejo de errores u otras condiciones excepcionales que podrían surgir durante la ejecución del trabajo, incluidas las restricciones sobre el uso de sistemas utilitarios; f) definir contactos de apoyo y de una instancia superior, incluidos los contactos de soporte externo, en el caso de dificultades operacionales o técnicas inesperadas; g) establecer las instrucciones sobre manejo de medios y elementos de salida, tales como el uso de papelería especial o la gestión de elementos de salida confidenciales, incluidos procedimientos para la disposición segura de elementos de salida de trabajos fallidos; h) definir los procedimientos de reinicio y recuperación del sistema para uso en el caso de falla del sistema; i) definir la gestión de la información de rastros de auditoría y de información del log del sistema; j) establecer los procedimientos de seguimiento.	Se cuenta un procedimiento para la gestión de las copias de respaldo;	Falta de los procedimientos de operación con instrucciones operacionales, los siguientes: a) instalar y configurar sistemas; b) establecer el procesamiento y manejo de información, tanto automático como manual; d) definir los requisitos de programación, incluidas las interdependencias con otros sistemas, los tiempos de finalización del primer y último trabajos; e) establecer las instrucciones para manejo de errores u otras condiciones excepcionales que podrían surgir durante la ejecución del trabajo, incluidas las restricciones sobre el uso de sistemas utilitarios; f) definir contactos de apoyo y de una instancia superior, incluidos los contactos de soporte externo, en el caso de dificultades operacionales o técnicas inesperadas; g) establecer las instrucciones sobre manejo de medios y elementos de salida, tales como el uso de papelería especial o la gestión de elementos de salida confidenciales, incluidos procedimientos para la disposición segura de elementos de salida de trabajos fallidos; h) definir los procedimientos de reinicio y recuperación del sistema para uso en el caso de falla del sistema; i) definir la gestión de la información de rastros de auditoría y de información del log del sistema; j) establecer los procedimientos de seguimiento.	0	

Cuadro 5. (Continuación)

			Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Técnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia							
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.4.1.2	Responsable de TICs	Gestión de cambios	Se debe controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	A.12.1.2		Revisar los procedimientos de control de cambios, que incluyen: a) Identificar y registrar los cambios significativos; b) Planificar y puesta a prueba de los cambios; c) Valorar los impactos potenciales, incluidos los impactos de estos cambios en la seguridad de la información; d) Tener un procedimiento de aprobación formal para los cambios propuestos; e) Verificar que se han cumplido los requisitos de seguridad de la información; f) Comunicar todos los detalles de los cambios a todas las personas pertinentes; g) Tener un procedimiento de apoyo, incluidos procedimientos y responsabilidades para abortar cambios no exitosos y recuperarse de ellos, y eventos no previstos; h) Contar con un suministro de un proceso de cambio de emergencia que posibilite la implementación rápida y controlada de los cambios necesarios para resolver un incidente.	No se tiene implementado		0	
T.4.1.3	Responsable de TICs	Gestión de capacidad	Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.	A.12.1.3		Revisar los procedimientos para la gestión de la demanda de capacidad, que incluyen: a) Eliminar datos obsoletos (espacio en disco); b) realizar cierre definitivo de aplicaciones, sistemas, bases de datos o ambientes; c) optimizar cronogramas y procesos de lotes; d) optimizar las consultas de bases de datos o lógicas de las aplicaciones; e) realizar una negación o restricción de ancho de banda a servicios ávidos de recursos, si estos no son críticos para el negocio (por ejemplo, video en tiempo real).	No se tiene implementado		0	
T.4.1.4	Responsable de TICs	Separación de los ambientes de desarrollo, pruebas y operación	Se debe separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	A.12.1.4		Revisar los procedimientos para la separación de ambientes, que incluyen: a) definir y documentar las reglas para la transferencia de software del estatus de desarrollo al de operaciones. b) establecer que el software de desarrollo y de operaciones debe funcionar en diferentes sistemas o procesadores de computador y en diferentes dominios o directorios; c) definir que los cambios en los sistemas operativos y aplicaciones se deben probar en un entorno de pruebas antes de aplicarlos a los sistemas operacionales; d) definir que solo en circunstancias excepcionales, las pruebas no se deben llevar a cabo en los sistemas operacionales; e) establecer que los compiladores, editores y otras herramientas de desarrollo o utilitarios del sistema no debe ser accesibles desde sistemas operacionales cuando no se requiere; f) establecer que los usuarios deben usar diferentes perfiles de usuario para sistemas operacionales y de pruebas, y los menús deben desplegar mensajes de identificación apropiados para reducir el riesgo de error; g) definir que los datos sensibles no se debe copiar en el ambiente del sistema de pruebas, a menos que se suministren controles equivalentes para el sistema de pruebas	No se tiene implementado		0	
T.4.2	**Responsable de SI**	**PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS**	**Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.**	**A.12.2**					0	

Cuadro 5. (Continuación)

			Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Técnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia							
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.4.2.1	**Responsable de SI**	Controles contra códigos maliciosos	Se debe implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	A.12.2.1	Modelo de madurez gestionado	Revisar las siguientes directrices: a) establecer una política formal que prohíba el uso de software no autorizado; b) implementar controles para evitar o detectar el uso de software no autorizado (listas blancas de aplicaciones); b) implementar controles para evitar o detectar el uso de sitios web malicioso o que se sospecha que lo son (listas negras); d) establecer una política formal para proteger contra riesgos asociados con la obtención de archivos y de software ya sea mediante redes externas o cualquier otro medio, indicando qué medidas externas se deben tomar; e) reducir las vulnerabilidades de las que pueda aprovecharse el software malicioso, (medio de la gestión de la vulnerabilidad técnica); f) llevar a cabo revisiones regulares del software y del contenido de datos de los sistemas que apoyan los procesos críticos del negocio; se debería investigar formalmente la presencia de archivos no aprobados o de enmiendas no autorizadas; g) instalar y actualizar software de detección y reparación del software malicioso en los computadores y medios como una medida de control, en forma rutinaria; el análisis realizado debería incluir: 1) el análisis de cualquier archivo recibido por la red o por cualquier forma de medio de almacenamiento, para detectar el software malicioso, antes de uso; 2) el análisis de los adjuntos y descargas de los correos electrónicos, para determinación del software malicioso antes de uso; este análisis se debería llevar a cabo en diferentes lugares, (los servidores de los correos electrónicos, en los computadores de escritorio) y cuando se ingresa a la red de la organización; el análisis de páginas web, para determinar el software malicioso; h) definir procedimientos y responsabilidades relacionadas con la protección contra el software malicioso en los sistemas, formación acerca del uso de dichos procedimientos, reporte y recuperación de ataques de software malicioso; i) preparar planes de continuidad del negocio apropiados, para la recuperación de ataques de software malicioso, incluidos todos los datos necesarios, copias de respaldo del software y disposiciones para recuperación; j) implementar procedimientos para recolectar información en forma regular, (la suscripción a listas de correos o la verificación de sitios web que suministran información acerca de nuevo software malicioso); k) implementar procedimientos para verificar información relacionada con el software malicioso, y asegurarse de que los boletines de advertencia sean exactos e informativos; l) alistar entornos en donde se pueden obtener impactos catastróficos.	No se tiene implementado		0	
T.4.3	**Responsable de TICs**	**COPIAS DE RESPALDO**	**Proteger contra la pérdida de datos.**	**A.12.3**	Modelo de madurez gestionado				20	

Cuadro 5. (Continuación)

			Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Técnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia							
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.4.4.1	Responsable de SI	Registro de eventos	Se debe elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	A.12.4.1	Modelo de madurez gestionado cuantitativamente	Revisar los registros de eventos que incluyan: a) identificar los usuarios; b) establecer las actividades del sistema; c) definir las fechas, horas y detalles de los eventos clave, (entrada y salida); d) identificar el dispositivo o ubicación, si es posible, e identificador del sistema; e) tener registros de intentos de acceso al sistema exitosos y rechazados; e) definir registros de datos exitosos y rechazados y otros intentos de acceso a recursos; g) establecer los cambios a la configuración del sistema; h) definir el uso de privilegios; i) establecer el uso de utilitarios y aplicaciones del sistema; j) definir los archivos a los que se tuvo acceso, y el tipo de acceso; k) establecer las direcciones y protocolos de red; l) definir las alarmas accionadas por el sistema de control de acceso; m) activar y desactivar los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusión; n) registrar las transacciones ejecutadas por los usuarios en las aplicaciones.	No se tiene implementado		0	
T.4.4.2	Responsable de SI	Protección de la información de registro	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	A.12.4.2		Revisar los procedimientos y controles dirigidos a proteger contra cambios no autorizados de la información del registro y contra problemas con la instalación de registro, que incluya: a) verificar todas las alteraciones a los tipos de mensaje que se registran; b) establecer los archivos log que son editados o eliminados; c) verificar cuando se excede la capacidad de almacenamiento del medio de archivo log, lo que da como resultado falla en el registro de eventos, o sobre escritura de eventos pasados registrados.	No se tiene implementado		0	
T.4.4.3	Responsable de SI	Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	A.12.4.3	Modelo de madurez gestionado cuantitativamente	Revisar los registros de las actividades del administrador y del operador del sistema, los registros se deben proteger y revisar con regularidad.	No se tiene implementado		0	
T.4.4.4	Responsable de SI	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	A.12.4.4		Revisar se deberían sincronizar con una única fuente de referencia de tiempo Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.	No se tiene implementado		0	

Cuadro 5. (Continuación)

			Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Técnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia							
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.4.5	**Responsable de TICs**	**CONTROL DE SOFTWARE OPERACIONAL**	**Asegurar la integridad de los sistemas operacionales.**	**A.12.5**	Modelo de madurez definido		No se tiene implementado		**0**	
T.4.5.1	Responsable de TICs	Instalación de software en sistemas operativos	Se debe implementar procedimientos para controlar la instalación de software en sistemas operativos.	A.12.5.1		Revisar las siguientes directrices para control de software operacional: a) actualizar el software operacional, aplicaciones y bibliotecas de programas solo la debe llevar a cabo administradores entrenados, con autorización apropiada de la dirección; b) definir que los sistemas operacionales sólo debe contener códigos ejecutables aprobados, no el código de desarrollo o compiladores; c) establecer que las aplicaciones y el software del sistema operativo solo se debe implementar después de pruebas extensas y exitosas; los ensayos deben abarcar la usabilidad, la seguridad, los efectos sobre otros sistemas y la facilidad de uso, y se debe llevar a cabo en sistemas separados; se debe asegurar que todas las bibliotecas de fuentes de programas correspondientes hayan sido actualizadas; d) usar un sistema de control de la configuración para mantener el control de todo el software implementado, al igual que la documentación del sistema; e) establecer una estrategia de retroceso (rol back) antes de implementar los cambios; f) mantener un log de auditoría de todas las actualizaciones de las bibliotecas de programas operacionales; g) definir las versiones anteriores del software de aplicación se deben conservar como una medida de contingencia; h) establecer que las versiones de software anteriores se deben llevar al archivo permanente, junto con toda la información y parámetros, procedimientos, detalles de configuración y software de soporte anteriores, en tanto los datos permanezcan en el archivo permanente.	No se tiene implementado		0	
T.4.6	**Responsable de SI**	**GESTIÓN DE LA VULNERABILIDAD TÉCNICA**	**Prevenir el aprovechamiento de las vulnerabilidades técnicas.**	**A.12.6**	Modelo de madurez gestionado				**20**	

Cuadro 5. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Técnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.4.6.1	Responsable de SI	Gestión de las vulnerabilidades técnicas	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	A.12.6.1		Revisar las siguientes directrices para vulnerabilidades técnicas: a) definir y establecer los roles y responsabilidades asociados con la gestión de la vulnerabilidad técnica, incluido el seguimiento de la vulnerabilidad, la valoración de riesgos de vulnerabilidad, la colocación de parches, el seguimiento de activos y cualquier responsabilidad de coordinación requerida; b) definir los recursos de información que se usarán para identificar las vulnerabilidades técnicas pertinentes y para mantener la toma de conciencia acerca de ellos se debe identificar para el software y otra tecnología; c) una línea de tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas pertinentes potencialmente; d) establecer que una vez que se haya identificado una vulnerabilidad técnica potencial, la organización debería identificar los riesgos asociados y las acciones por tomar; esta acción puede involucrar la colocación de parches de sistemas vulnerables o la aplicación de otros controles; Si no es posible colocar controles se deben documentar en los riesgos de acuerdo a su probabilidad e impacto y colocarlo como riesgo aceptado. e) definir dependiendo de la urgencia con la que se necesite tratar una vulnerabilidad técnica, la acción tomada se debería llevar a cabo de acuerdo con los controles relacionados con la gestión de cambios, o siguiendo los procedimientos de respuesta a incidentes de seguridad de la información; f) establecer, si está disponible un parche de una fuente legítima, se debe valorar los riesgos asociados con la instalación del parche (los riesgos que acarrea la vulnerabilidad se debe comparar con el riesgo de instalar el parche); g) establecer que los parches se deben probar y evaluar antes de su instalación, para asegurarse de que son eficaces y no producen efectos secundarios que no se puedan tolerar; si no hay parches disponibles, se debe considerar otros controles como: 1) dejar de operar los servicios o capacidades relacionados con la vulnerabilidad; 2) adaptar o adicionar controles de acceso, (cortafuegos, en los límites de la red); 3) incrementar el seguimiento para detectar ataques reales; 4) tomar conciencia sobre la vulnerabilidad; h) llevar un log de auditoría para todos los procedimientos realizados; i) hacer seguimiento y evaluación regulares del proceso de gestión de vulnerabilidad técnica, con el fin de asegurar su eficacia y eficiencia; j) abordar primero los sistemas que están en alto riesgo; k) establecer un proceso de gestión eficaz de la vulnerabilidad técnica alineada con las actividades de gestión de incidentes para comunicar los datos sobre vulnerabilidades a la función de respuesta a incidentes y suministrar los procedimientos técnicos para realizarse si llegara a ocurrir un incidente; l) definir un procedimiento para hacer frente a una situación en la que se ha identificado una vulnerabilidad, pero no hay una contramedida adecuada. En esta situación, la organización debería evaluar los riesgos relacionados con la vulnerabilidad conocida y definir las acciones de detección y correctivas apropiadas.	No se tiene implementado		0	
T.4.6.2	Responsable de TICs	Restricciones sobre la instalación de software	Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	A.12.6.2		Revisar las restricciones y las reglas para la instalación de software por parte de los usuarios.	Se tiene establecido en la Política de seguridad de la información una regla además se cuenta con una herramienta de seguridad (PCSECURE) que maneja esta restricción		40	

Cuadro 5. (Continuación)

			Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Técnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia							
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.4.7	**Responsable de TICs**	**CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN**	**Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.**	**A.12.7**					0	
T.4.7.1	Responsable de TICs	Controles sobre auditorías de sistemas de información	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se debe planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	A.12.7.1		Revisar las siguientes directrices para las auditorias de sistemas de información: a) establecer los requisitos de auditoría para acceso a sistemas y a datos se debe acordar con la dirección apropiada; b) definir el alcance de las pruebas técnicas de auditoría se debe acordar y controlar; c) establecer las pruebas de auditoría se debe limitar a acceso a software y datos únicamente para lectura; d) definir el acceso diferente al de solo lectura solamente se debe prever para copias aisladas de los archivos del sistema, que se deben borrar una vez que la auditoría haya finalizado, o se debe proporcionar información apropiada si hay obligación de mantener estos archivos bajo los requisitos de documentación de auditoría; e) definir los requisitos para procesos especiales y adicionales se debe identificar y acordar; f) establecer las pruebas de auditoría que puedan afectar la disponibilidad del sistema se deben realizar fuera de horas laborales; g) hacer seguimiento de todos los accesos y logged para producir un rastro de referencia.	No se tiene implementado		0	
T.5	**Responsable de TICs/Responsable de SI**	**SEGURIDAD DE LAS COMUNICACIONES**		**A.13**					0	
T.5.1	**Responsable de TICs**	**GESTIÓN DE LA SEGURIDAD DE LAS REDES**	**Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.**	**A.13.1**			No se tiene implementado		**0**	
T.5.1.1	Responsable de TICs	Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	A.13.1.1		Revisar las siguientes directrices para la gestión de seguridad de redes: a) establecer las responsabilidades y procedimientos para la gestión de equipos de redes; b) definir la responsabilidad operacional por las redes se debería separar de las operaciones informáticas, en donde sea apropiado; c) establecer controles especiales para salvaguardar la confidencialidad e integridad de los datos que pasan sobre redes públicas o sobre redes inalámbricas, y para proteger los sistemas y aplicaciones conectados; d) De acuerdo a NIST, Gestionar el acceso remoto d) aplicar logging y seguimiento adecuados para posibilitar el registro y detección de acciones que pueden afectar, o son pertinentes a la seguridad de la información; e) definir las actividades de gestión a coordinar estrechamente tanto para optimizar el servicio de la organización, como para asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información; f) establecer los sistemas en la red que se autenticar; g) restringir la conexión de los sistemas a la red.	No se tiene implementado		0	

Cuadro 5. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (técnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.5.1.2	Responsable de SI	Seguridad de los servicios de red	Se debe identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	A.13.1.2		Revisar las siguientes directrices para la seguridad de los servicios de red: a) establecer la tecnología aplicada a la seguridad de servicios de red, tales como autenticación, encriptación y controles de conexión de red; b) definir los parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad y de red; c) establecer los procedimientos para el uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red, cuando sea necesario.	No se tiene implementado		0	
T.5.1.3	Responsable de TICs	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	A.13.1.3		De acuerdo a NIST se debe proteger la integridad de las redes incorporando segregación donde se requiera.	No se tiene implementado		0	
T.5.2	**Responsable de TICs**	**TRANSFERENCIA DE INFORMACIÓN**	**Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.**	**A.13.2**			Todo tipo de intercambio de información o de acceso a los activos de información de la Entidad a algún tercero se debe realizar a través de convenios ínter-administrativos o de acuerdos de cualquier índole, los demás criterios del control no se tienen implementados		**0**	
T.5.2.1	Responsable de TICs	Políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.	A.13.2.1		De acuerdo a la NIST: Se deben mapear los flujos de comunicaciones y datos para poder cumplir con este ítem. Revisar las siguientes directrices: a) definir los procedimientos diseñados para proteger la información transferida contra interceptación, copiado, modificación, enrutado y destrucción; b) definir los procedimientos para la detección de software malicioso y protección contra éste, que puede ser transmitido mediante el uso de comunicaciones electrónicas; c) definir los procedimientos para proteger información electrónica sensible comunicada que están como adjuntos; d) establecer la política o directrices que presentan el uso aceptable de las instalaciones de comunicación; e) definir las responsabilidades del personal, las partes externas y cualquier otro usuario no comprometen a la organización, (por difamación, acoso, suplantación, envío de cadenas, compras no autorizadas, etc.); f) establecer el uso de técnicas criptográficas, (proteger la confidencialidad, la integridad y la autenticidad de la información). g) establecer las directrices sobre retención y disposición para toda la correspondencia del negocio, incluidos mensajes, de acuerdo con la legislación y reglamentaciones locales y nacionales; h) definir los controles y restricciones asociadas con las instalaciones de comunicación, (el reenvío automático de correo electrónico a direcciones de correo externas); i) brindar asesoría al personal para que tome las precauciones apropiadas acerca de no revelar información confidencial; j) no dejar mensajes que contengan información confidencial, en las máquinas contestadoras, ya que éstos pueden ser escuchados por personas no autorizadas, almacenados en sistemas comunales o almacenados incorrectamente como resultado de una marcación incorrecta; k) brindar asesoría al personal acerca de los problemas de usar máquinas o servicios de fax, a saber: 1) acceso no autorizado a almacenes de mensajes built-in para recuperar mensajes; 2) programar las máquinas en forma deliberada o accidental para enviar mensajes a números específicos; enviar documentos y mensajes a un número equivocado, ya sea por marcación errada o por marcar un número almacenado equivocado.	No se tiene implementado		0	

Cuadro 5. (Continuación)

			Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Técnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia							
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.5.2.2	Responsable de TICs	Acuerdos sobre transferencia de información	Los acuerdos deben tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.	A.13.2.2		Revisar las siguientes directrices para transferencia segura de la información: a) establecer las responsabilidades de la dirección para controlar y notificar la transmisión, despacho y recibo; b) definir los procedimientos para asegurar trazabilidad y no repudio; c) definir los estándares técnicos mínimos para empaquetado y transmisión; d) tener certificados de depósito de títulos en garantía; e) establecer los estándares de identificación de mensajería; f) definir las responsabilidades y obligaciones en el caso de incidentes de seguridad de la información, tales como pérdidas de datos; g) establecer el uso de un sistema de etiquetado acordado para información sensible o crítica, que asegure que el significado de la etiqueta se entiende de inmediato, y que la información está protegida apropiadamente; h) definir las normas técnicas para registro y lectura de información y software; i) cualquier control especial que se requiera para proteger elementos críticos, tales como criptografía; j) mantener una cadena de custodia para la información mientras está en tránsito; k) definir los niveles aceptables de control de acceso.	No se tiene implementado		0	
T.5.2.3	Responsable de TICs	Mensajería electrónica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	A.13.2.3		Revisar las siguientes directrices para mensajería electrónica: a) definir la protección de mensajes contra acceso no autorizado, modificación o denegación del servicio proporcionales al esquema de clasificación adoptado por la organización; b) asegurar el direccionamiento y transporte correctos del mensaje; c) establecer la confiabilidad y disponibilidad del servicio; d) definir las consideraciones legales, (los requisitos para firmas electrónicas; e) establecer la obtención de aprobación antes de usar servicios públicos externos como mensajería instantánea, redes sociales o intercambio de información); f) definir niveles más fuertes de autenticación para control del acceso desde redes accesibles públicamente.	No se tiene implementado		0	
T.5.2.4	Responsable de SI	Acuerdos de confidencialidad o de no divulgación	Se debe identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	A.13.2.4		Revisar las siguientes directrices para acuerdos de confidencialidad: a) definir la información que se va a proteger (información confidencial); b) determinar la duración esperada de un acuerdo, incluidos los casos en los que podría ser necesario mantener la confidencialidad indefinidamente; c) establecer las acciones requeridas cuando termina el acuerdo; d) definir las responsabilidades y acciones de los firmantes para evitar la divulgación no autorizada de información; e) definir la propiedad de la información, los secretos comerciales y la propiedad intelectual, y cómo esto se relaciona con la protección de información confidencial; f) definir el uso permitido de información confidencial y los derechos del firmante para usar la información; g) establecer el derecho a actividades de auditoría y de seguimiento que involucran información confidencial; h) definir el proceso de notificación y reporte de divulgación no autorizada o fuga de información confidencial; i) definir los plazos para que la información sea devuelta o destruida al cesar el acuerdo; j) establecer las acciones que se espera tomar en caso de violación del acuerdo.	No se tiene implementado		0	
T.6	**Responsable de SI/Responsable de TICs**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**		**A.14**					**1**	

Cuadro 5. (Continuación)

	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Técnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia									
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.6.1	**Responsable de SI**	**REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN**	**Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.**	**A.14.1**			En estudios previos para la contratación se revisan los requerimiento mínimos técnicos, funcionales y de seguridad de las adquisiciones, , sin embargo también de debe estructurar procedimientos donde se especifique los requisitos para la Adquisición e Implementación de los Sistemas de Información y actualizar el manual de contratación		**0**	
T.6.1.1	Responsable de SI	Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	A.14.1.1		Revisar las siguientes directrices para análisis y especificaciones de requisitos de seguridad de la información: a) establecer el nivel de confianza requerido con relación a la identificación declarada de los usuarios, para obtener los requisitos de autenticación de usuario. b) definir los procesos de suministro de acceso y de autorización para usuarios del negocio, al igual que para usuarios privilegiados o técnicos; c) informar a los usuarios y operadores sobre sus deberes y responsabilidades; d) definir las necesidades de protección de activos involucrados, en particular acerca de disponibilidad, confidencialidad, integridad; e) definir los requisitos obtenidos de los procesos del negocio, tales como los requisitos de ingreso y seguimiento, y de no repudio; f) establecer los requisitos exigidos por otros controles de seguridad, (interfaces con el ingreso o seguimiento, o los sistemas de detección de fuga de datos).	No se tiene implementado		0	
T.6.1.2	Responsable de SI	Seguridad de servicios de las aplicaciones en redes públicas	La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	A.14.1.2		Revisar las siguientes directrices para la seguridad de servicios de las aplicaciones en redes públicas: a) definir el nivel de confianza que cada parte requiere con relación a la identidad declarada por la otra parte, (por medio de autenticación); b) establecer los procesos de autorización asociados con quien puede aprobar el contenido o expedir o firmar documentos transaccionales clave; c) asegurar que los socios de comunicación estén completamente informados de sus autorizaciones para suministro o uso del servicio; d) determinar y cumplir los requisitos para confidencialidad, integridad, prueba de despacho y recibo de documentos clave y el no repudio de los contratos, (asociados con procesos de ofertas y contratos); e) definir el nivel de confianza requerido en la integridad de los documentos clave; f) establecer los requisitos de protección de cualquier información confidencial; g) definir la confidencialidad e integridad de cualquier transacción de pedidos, información de pagos, detalles de la dirección de entrega y confirmación de recibos; h) definir el grado de verificación apropiado de la información de pago suministrada por un cliente; i) seleccionar la forma de arreglo de pago más apropiado para protegerse contra fraude; j) definir el nivel de protección requerido para mantener la confidencialidad e integridad de la información del pedido; k) evitar la pérdida o duplicación de información de la transacción; l) definir la responsabilidad civil asociada con cualquier transacción fraudulenta; m) establecer los requisitos de seguros. n) De acuerdo a NIST se deben usar mecanismos de chequeo de las integridad para verificar la integridad del software, firmware, e información			0	

Cuadro 5. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Técnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.6.1.3	Responsable de SI	Protección de transacciones de los servicios de las aplicaciones	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	A.14.1.3		Revisar las siguientes directrices protección de transacciones de los servicios de las aplicaciones: a) definir el uso de firmas electrónicas por cada una de las partes involucradas en la transacción; b) establecer todos los aspectos de la transacción, es decir, asegurar que: 1) definir la información de autenticación secreta de usuario, de todas las partes, se valide y verifique; 2) definir a transacción permanezca confidencial; 3) mantener la privacidad asociada con todas las partes involucradas; c) definir la trayectoria de las comunicaciones entre todas las partes involucradas esté encriptada; d) definir los protocolos usados para comunicarse entre todas las partes involucradas estén asegurados; e) asegurar que el almacenamiento de los detalles de la transacción esté afuera de cualquier entorno accesible públicamente, (en una plataforma de almacenamiento existente en la intranet de la organización, y no retenido ni expuesto en un medio de almacenamiento accesible directamente desde Internet); f) utilizar una autoridad confiable (para los propósitos de emitir y mantener firmas digitales o certificados digitales), la seguridad está integrada e incluida en todo el proceso de gestión de certificados/firmas de un extremo a otro.	Se tiene implementado el uso de firmas digitales para protección de transacciones de los servicios de las aplicaciones, se cumplen con los controles, protocolos y directrices entre las partes involucradas tales como Ministerio de Hacienda y Crédito Público, Bancos, Superintendencia Nacional de Salud, se maneja Red de Alta velocidad del Gobierno Colombiano - RAVEC permite compartir e intercambiar información, realizar procesos y actividades conjuntas; posibilita el desarrollo y ejecución de proyectos estatales relacionados con trámites, servicios en línea y comercio electrónico; optimizando los servicios al ciudadano		0	
T.6.2	**Responsable de SI**	**SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE**	**Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.**	**A.14.2**	Modelo de madurez definido		No se tiene procedimiento de Implementación de los Sistemas de Información, donde se establezcan algunos controles para validación de los datos de entrada y procesamiento aplicando los modelos de pruebas técnicas, funcionales y de seguridad que sean necesarios.		**2**	
T.6.2.1	Responsable de SI	Política de desarrollo seguro	Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.	A.14.2.1		Revisar las siguientes directrices política de desarrollo seguro: a) definir la seguridad del ambiente de desarrollo; b) orientar la seguridad en el ciclo de vida de desarrollo del software: 1) definir la seguridad en la metodología de desarrollo de software; 2) establecer las directrices de codificación seguras para cada lenguaje de programación usado; c) definir los requisitos de seguridad en la fase diseño; d) definir los puntos de chequeo de seguridad dentro de los hitos del proyecto; e) establecer los depósitos seguros; f) definir la seguridad en el control de la versión; g) establecer el conocimiento requerido sobre seguridad de la aplicación; h) definir la capacidad de los desarrolladores para evitar, encontrar y resolver las vulnerabilidades.	No se tiene implementado		0	

Cuadro 5. (Continuación)

			Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Técnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia							
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.6.2.2	Responsable de TICs	Procedimientos de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	A.14.2.2		Revisar las siguientes directrices procedimientos control de cambio en sistemas: a) llevar un registro de los niveles de autorización acordados; b) asegurar que los cambios se presenten a los usuarios autorizados; c) revisar los controles y procedimientos de integridad para asegurar que no se vean comprometidos por los cambios; d) identificar todo el software, información, entidades de bases de datos y hardware que requieren corrección; e) identificar y verificar el código crítico de seguridad para minimizar la posibilidad de debilidades de seguridad conocidas; f) obtener aprobación formal para propuestas detalladas antes de que el trabajo comience; g) revisar antes de la implementación, asegurar que los usuarios autorizados aceptan los cambios; h) asegurar que el conjunto de documentación del sistema está actualizado al completar cada cambio, y que la documentación antigua se lleva al archivo permanente, o se dispone de ella; i) mantener un control de versiones para todas las actualizaciones de software; j) mantener un rastro de auditoría de todas las solicitudes de cambio; k) asegurar que la documentación de operación y los procedimientos de los usuarios experimenten los cambios que les permitan seguir siendo apropiados; l) asegurar que la implementación de los cambios ocurre en el momento correcto y no afecta los procesos de negocio involucrados.	No se tiene implementado		0	
T.6.2.3	Responsable de TICs	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	A.14.2.3		Revisar las siguientes directrices revisión técnica de las aplicaciones después de cambios en la plataforma de operación: a) revisar los procedimientos de integridad y control de aplicaciones para asegurar que no estén comprometidos debido a los cambios en las plataformas de operaciones; b) asegurar que la notificación de los cambios en la plataforma operativa se hace a tiempo para permitir las pruebas y revisiones apropiadas antes de la implementación; c) asegurar que se hacen cambios apropiados en los planes de continuidad del negocio.			0	
T.6.2.4	Responsable de TICs	Restricciones en los cambios a los paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	A.14.2.4		Revisar las siguientes directrices restricciones en los cambios a los paquetes de software: a) definir el riesgo de que los procesos de integridad y los controles incluidos se vean comprometidos; b) obtener el consentimiento del vendedor; c) obtener del vendedor los cambios requeridos, a medida que se actualiza el programa estándar; d) evaluar el impacto, si la organización llega a ser responsable del mantenimiento futuro del software como resultado de los cambios; e) definir la compatibilidad con otro software en uso.	se manejan en acuerdo con los términos del Contrato		20	
T.6.2.5	Responsable de TICs	Principios de construcción de sistemas seguros	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	A.14.2.5		Revisar la documentación y los principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	No se tiene implementado		0	

Cuadro 5. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Técnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.6.2.6	Responsable de TICs	Ambiente de desarrollo seguro	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	A.14.2.6		Revisar las siguientes directrices para ambiente de desarrollo seguro: a) carácter sensible de los datos que el sistema va a procesar, almacenar y transmitir; b) definir los requisitos externos e internos aplicables, (reglamentaciones o políticas); c) definir los controles de seguridad ya implementados por la organización, que brindan soportar al desarrollo del sistema; d) establecer la confiabilidad del personal que trabaja en el ambiente; e) definir el grado de contratación externa asociado con el desarrollo del sistema; f) definir la necesidad de separación entre diferentes ambientes de desarrollo; g) definir el control de acceso al ambiente de desarrollo; h) establecer el seguimiento de los cambios en el ambiente y en los códigos almacenados ahí; i) definir las copias de respaldo se almacenan en lugares seguros fuera del sitio; j) definir el control sobre el movimiento de datos desde y hacia el ambiente.	No se tiene implementado		0	
T.6.2.7	Responsable de TICs	Desarrollo contratado externamente	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	A.14.2.7		Revisar las siguientes directrices desarrollo contratado externamente: a) definir los acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual relacionados con el contenido contratado externamente; b) establecer los requisitos contractuales para prácticas seguras de diseño, codificación y pruebas; c) definir el suministro del modelo de amenaza aprobado, al desarrollador externo; d) realizar los ensayos de aceptación para determinar la calidad y exactitud de los entregables; e) definir la evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad; f) definir la evidencia de que se han hecho pruebas suficientes para proteger contra contenido malicioso intencional y no intencional en el momento de la entrega; g) definir la evidencia de que se han hecho pruebas suficientes para proteger contra la presencia de vulnerabilidades conocidas; h) definir los certificados de depósito de títulos en garantía; (el código fuente ya no está disponible); i) establecer el derecho contractual con relación a procesos y controles de desarrollo de auditorías; j) documentar eficaz del ambiente de construcción usado para crear entregables; k) establecer que la organización es responsable de la conformidad con las leyes aplicables y con la verificación de la eficiencia del control.	Procedimiento APAJUOAJPT12 Supervisión de contratos	No se tiene: e) definir la evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad; f) definir la evidencia de que se han hecho pruebas suficientes para proteger contra contenido malicioso intencional y no intencional en el momento de la entrega; g) definir la evidencia de que se han hecho pruebas suficientes para proteger contra la presencia de vulnerabilidades conocidas;	0	
T.6.2.8	Responsable de SI	Pruebas de seguridad de sistemas	Durante el desarrollo se debe llevar a cabo pruebas de funcionalidad de la seguridad.	A.14.2.8	Modelo de madurez gestionado cuantitativamente	Verifique en una muestra que para pasar a producción los desarrollos se realizan pruebas de seguridad. También verifique que los procesos de detección de incidentes son probados periódicamente.	No se tiene implementado		0	

Cuadro 5. (Continuación)

	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Técnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia									
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.6.2.9	Responsable de TICs	Prueba de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se debe establecer programas de prueba para aceptación y criterios de aceptación relacionados.	A.14.2.9		Revisar las pruebas de aceptación de sistemas, para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.	Se establece dentro de los contratos		0	
T.6.3	Responsable de SI	**DATOS DE PRUEBA**	**Asegurar la protección de los datos usados para pruebas.**	**A.14.3**	Modelo de madurez definido		No se tiene procedimiento de Implementación de los Sistemas de Información, donde se establezcan algunos controles para validación de los datos de entrada y procesamiento aplicando los modelos de pruebas técnicas, funcionales y de seguridad que sean necesarios.		**0**	
T.6.3.1	Responsable de SI	Protección de datos de prueba	Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.	A.14.3.1		Revisar las siguientes directrices para protección de datos de prueba: a) establecer los procedimientos de control de acceso, que se aplican a los sistemas de aplicación operacionales, se debe aplicar también a los sistemas de aplicación de pruebas; b) tener una autorización separada cada vez que se copia información operacional a un ambiente de pruebas; c) definir que la información operacional se debe borrar del ambiente de pruebas inmediatamente después de finalizar las pruebas; d) establecer que el copiado y uso de la información operacional se debe logged para suministrar un rastro de auditoría.	No se tiene implementado		0	
T.7.	**Responsable de SI/Responsable de TICs**	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**		**A.16**					20	
T.7.1	**Responsable de SI**	**GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN**	**Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.**	**A.16.1**					20	

Cuadro 5. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Técnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.7.1.1	Responsable de SI	Responsabilidades y procedimientos	Se debe establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	A.16.1.1		Revisar las siguientes directrices responsabilidades y procedimientos: a) establecer las responsabilidades de gestión, para asegurar que los siguientes procedimientos se desarrollan y comunican adecuadamente dentro de la organización: 1) los procedimientos para la planificación y preparación de respuesta a incidentes; 2) los procedimientos para seguimiento, detección, análisis y reporte de eventos e incidentes de seguridad de la información; 3) los procedimientos para logging las actividades de gestión de incidentes; 4) los procedimientos para el manejo de evidencia forense; 5) los procedimientos para la valoración y toma de decisiones sobre eventos de seguridad de la información y la valoración de debilidades de seguridad de la información; 6) los procedimientos para respuesta, incluyendo aquellos para llevar el asunto a una instancia superior, recuperación controlada de un incidente y comunicación a personas u organizaciones internas y externas; b) establecer los procedimientos para asegurar que: 1) el personal competente maneje las cuestiones relacionadas con incidentes de seguridad de la información dentro de la organización; 2) se implemente un punto de contacto para la detección y reporte de incidentes de seguridad; 3) se mantengan contactos apropiados con las autoridades, grupos de interés o foros externos que manejen las cuestiones relacionadas con incidentes de seguridad de la información; c) definir el reporte de procedimientos debería incluir: 1) la preparación de formatos de reporte de eventos de seguridad de la información para apoyar la acción de reporte y ayudar a la persona que reporta a recordar todas las acciones necesarias en caso de un evento de seguridad de la información; 2) el procedimiento que se va a seguir en el caso de un evento de seguridad de la información, (tomar nota inmediatamente de todos los detalles, tales como el tipo de no conformidad o violación, mal funcionamiento, mensajes en la pantalla y reporte inmediato al punto de contacto y realizar solamente acciones coordinadas); 3) referencia a un proceso disciplinario formal establecido para ocuparse de los empleados que cometen violaciones a la seguridad; 4) los procesos de retroalimentación adecuados para asegurar que las personas que reportan eventos de seguridad de la información sean notificadas de los resultados después de que la cuestión haya sido tratada y cerrada.	No se tiene procedimiento implementado, este se cuenta en diseño		20	
T.7.1.2	Responsable de SI	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	A.16.1.2	Modelo de madurez definido	Revisar las siguientes directrices reporte de eventos de seguridad de la información: a) establecer un control de seguridad ineficaz; b) definir la violación de la integridad, confidencialidad o expectativas de disponibilidad de la información; c) definir los errores humanos; d) definir las no conformidades con políticas o directrices; e) definir las violaciones de acuerdos de seguridad física; f) establecer los cambios no controlados en el sistema; g) definir mal funcionamiento en el software o hardware; h) definir violaciones de acceso. **Tenga en cuenta para la calificación:** 1) Si se elaboran informes de TODOS los incidentes de seguridad y privacidad de la información, TODOS están documentados e incluidos en el plan de mejoramiento continuo. Se definen los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro, están en 40. 2) Si los controles y medidas identificados para disminuir los incidentes fueron implementados, están en 60.	No se tiene procedimiento implementado, este se cuenta en diseño		20	
T.7.1.3	Responsable de SI	Reporte de debilidades de seguridad de la información	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	A.16.1.3		Observe si los eventos son reportados de forma consistente en toda la entidad de acuerdo a los criterios establecidos.	No se tiene procedimiento implementado, este se cuenta en diseño		20	

Cuadro 5. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Técnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.7.1.4	Responsable de SI	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	A.16.1.4		Revise si los eventos de SI detectados son analizados para determinar si constituyen un incidente de seguridad de la información y entender los objetivos del ataque y sus métodos. Evidencia si los incidentes son categorizados y se cuenta con planes de respuesta para cada categoría.	No se tiene procedimiento implementado, este se cuenta en diseño		20	
T.7.1.5	Responsable de SI	Respuesta a incidentes de seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	A.16.1.5	Modelo de madurez gestionado cuantitativamente	Revisar las siguientes directrices para respuesta a incidentes de seguridad de la información: a) Los incidentes son contenidos y la probabilidad de que vuelvan a ocurrir mitigada. b) Se debe contar con un plan de recuperación de incidentes durante o después del mismo. b) recolectar evidencia lo más pronto posible después de que ocurra el incidente; c) llevar a cabo análisis forense de seguridad de la información, según se requiera d) llevar el asunto a una instancia superior, según se requiera; e) asegurar que todas las actividades de respuesta involucradas se registren adecuadamente para análisis posterior; f) comunicar la existencia del incidente de seguridad de la información o de cualquier detalle pertinente a él, al personal interno o externo a las organizaciones que necesitan saberlo; g) tratar las debilidades de seguridad de información que se encontraron que causan o contribuyen al incidente; g) establecer que una vez que el incidente se haya tratado lo suficiente, cerrarlo formalmente y hacer un registro de esto. h) de acuerdo a la NIST se deben investigar las notificaciones de los sistemas de detección. **Tenga en cuenta para la calificación:** 1) Si los planes de respuesta a incidentes incluyen algunas áreas de la entidad y si se evalúa la efectividad los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro es 60 2) Se incluyen todas las áreas de la Entidad, en los planes de respuesta de incidentes es 80	No se tiene procedimiento implementado, este se cuenta en diseño	Revisar las siguientes directrices para respuesta a incidentes de seguridad de la información: a) Los incidentes son contenidos y la probabilidad de que vuelvan a ocurrir mitigada. b) Se debe contar con un plan de recuperación de incidentes durante o después del mismo. b) recolectar evidencia lo más pronto posible después de que ocurra el incidente; c) llevar a cabo análisis forense de seguridad de la información, según se requiera d) llevar el asunto a una instancia superior, según se requiera; e) asegurar que todas las actividades de respuesta involucradas se registren adecuadamente para análisis posterior; f) comunicar la existencia del incidente de seguridad de la información o de cualquier detalle pertinente a él, al personal interno o externo a las organizaciones que necesitan saberlo; g) tratar las debilidades de seguridad de información que se encontraron que causan o contribuyen al incidente; g) establecer que una vez que el incidente se haya tratado lo suficiente, cerrarlo formalmente y hacer un registro de esto. h) de acuerdo a la NIST se deben investigar las notificaciones de los sistemas de detección. **Tenga en cuenta para la calificación:** 1) Si los planes de respuesta a incidentes incluyen algunas áreas de la entidad y si se evalúa la efectividad los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro es 60 2) Se incluyen todas las áreas de la Entidad, en los planes de respuesta de incidentes es 80	No se tiene procedimiento implementado, este se cuenta en diseño	

Cuadro 5. (Continuación)

			Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Técnicas) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia							
ID. ITEM	**CARGO**	**ITEM**	**DESCRIPCIÓN**	**ISO**	**MSPI**	**PRUEBA**	**EVIDENCIA**	**BRECHA**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**	**RECOMENDACIÓN**
T.7.1.6	Responsable de TICs	Aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	A.16.1.6	Modelo de madurez gestionado cuantitativamente	De acuerdo a la NIST se debe entender cuál fue el impacto del incidente. Las lecciones aprendidas deben ser usadas para actualizar los planes de respuesta a los incidentes de SI. **Tenga en cuenta para la calificación:** La Entidad aprende continuamente sobre los incidentes de seguridad presentados.	No se tiene procedimiento implementado, este se cuenta en diseño		20	
T.7.1.7	Responsable de TICs	Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	A.16.1.7	Modelo de madurez gestionado Modelo de madurez definido	Revisar las siguientes directrices para recolección de evidencia: a) definir la cadena de custodia; b) establecer la seguridad de la evidencia; c) definir la seguridad del personal; d) definir los roles y responsabilidades del personal involucrado; e) establecer la competencia del personal; f) realizar la documentación; g) definir las sesiones informativas.	No se tiene procedimiento implementado, este se cuenta en diseño		20	

Fuente: Instrumento de evaluación del MINTIC

Cuadro 6. Planear, hacer, verificar y actuar

			Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (PHVA) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia							
COMPONENTE	ID	CARGO	ÍTEM	DESCRIPCIÓN	PRUEBA	MSPI	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO PHVA	RECOMENDACIÓN
PLANIFICACIÓN	P.1	Responsable SI	Alcance MSPI (Modelo de Seguridad y Privacidad de la Información)	Se debe determinar los límites y la aplicabilidad del SGSI para establecer su alcance.	Solicite el documento del alcance que debe estar aprobado, socializado al interior de la Entidad, por la alta dirección. Determine si en la definición del alcance se considera: 1) Aspectos internos y externos referidos en el 4.1.: La Entidad debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito y que afectan su capacidad para lograr los resultados previstos en el SGSI. Nota. La terminación de estos aspectos hace referencia a establecer el contexto interno y externo de la empresa, referencia a la norma ISO 31000:2009 en el apartado 5.3. 2) Los requisitos referidos en 4.2.: a. Se debe determinar las partes interesadas que son pertinentes al SGSI. b. Se debe determinar los requisitos de las partes interesadas. Nota. Los requisitos pueden incluir los requisitos legales y de reglamentación y las obligaciones contractuales. 3) Las interfaces y dependencias entre las actividades realizadas y las que realizan otras entidades del gobierno nacional o entidades exteriores	Componente planificación	Borrador en Word incluido en el Manual del Sistema de Gestión de la Seguridad y P Privacidad de la Información	No se encuentra aprobada	20	
	P.2		Políticas de seguridad y privacidad de la información	Se debe definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y comunicada a los empleados y a la partes externas pertinentes	Solicite la política de seguridad de la información de la entidad y evalúe: a) Si se definen los objetivos, alcance de la política b) Si esta se encuentra alineada con la estrategia y objetivos de la entidad c) Si fue debidamente aprobada y socializada al interior de la entidad por la alta dirección Revise si la política: a)Define que es seguridad de la información b) La asignación de las responsabilidades generales y específicas para la gestión de la seguridad de la información, a roles definidos; c) Los procesos para manejar las desviaciones y las excepciones. Indague sobre los responsables designados formalmente por la dirección para desarrollar, actualizar y revisar las políticas. Verifique cada cuanto o bajo qué circunstancias se revisan y actualizan, verifique la última fecha de emisión de la política frente a la fecha actual y que cambios a sufrido, por lo menos debe haber una revisión anual. Para la calificación tenga en cuenta que: 1) Si se empiezan a definir las políticas de seguridad y privacidad de la información basada en el Modelo de Seguridad y Privacidad de la Información, están en 20. 2) Si se revisan y se aprueban las políticas de seguridad y privacidad de la información, están en 40. 3) Si se divulgan las políticas de seguridad y privacidad de la información, están en 60.	componente planificación		Dentro de la política no se define que es seguridad de la información. No se tiene asignación de las responsabilidades generales y específicas para la gestión de la seguridad de la información, a roles definidos. No se tienen los procesos para manejar las desviaciones y excepciones.	40	Actualizar la política subsanando las brechas descritas
						componente planificación		Se creó en la fecha: 27 de agosto de 2014, se tiene una actualización de fecha: 31 de agosto de 2016 sin embargo esta no ha sido aprobada.	20	Una vez actualizada la política, establecer cada cuanto se debe realizar revisión y actualización de la misma.

Cuadro 6. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (PHVA) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia								vive digital para la gente	
COMPONENTE	ID	CARGO	ÍTEM	DESCRIPCIÓN	PRUEBA	MSPI	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO PHVA	RECOMENDACIÓN
PLANIFICACIÓN	P.3	Calidad	Procedimientos de control documental del MSPI	La información documentada se debe controlar para asegurar que: a. Esté disponible y adecuado para su uso, cuando y donde se requiere b. Esté protegida adecuadamente.	Solicite Formatos de procesos y procedimientos debidamente definidos, establecidos y aprobados por el comité que integre los sistemas de gestión institucional, por ejemplo el sistema de calidad SGC. Verifique: 1) Cómo se controla su distribución, acceso, recuperación y uso 2) Cómo se almacena y se asegura su preservación 3) Cómo se controlan los cambios	componente planificación			0	
	P.4	Responsable SI	Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información	Solicite el acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (ó e que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección. Revise la estructura del SGSI: 1) ¿Tiene el SGSI suficiente apoyo de la alta dirección?, esto se ve reflejado en comités donde se discutan temas como la política de SI, los riesgos o incidentes. 2) ¿Están claramente definidos los roles y responsabilidades y asignados a personal con las competencias requeridas?, 3) ¿Están identificadas los responsables y responsabilidades para la protección de los activos? (Una práctica común es nombrar un propietario para cada activo, quien entonces se convierte en el responsable de su protección) 4¿) Están definidas las responsabilidades para la gestión del riesgo de SI y la aceptación de los riesgos residuales? 5) ¿Están definidos y documentados los niveles de autorización? 6) Se cuenta con un presupuesto formalmente asignado a las actividades del SGSI (por ejemplo campañas de sensibilización en seguridad de la información)	componente planificación		Dentro del borrador no se tienen los roles frente a la ciberseguridad establecidos, Teniendo en cuenta que el documento es un borrador hay roles que no se han socializado formalmente, no se tiene claridad en los roles y responsabilidades para la detección de incidentes. El acto administrativo define el comité como tal, sin embargo a la fecha, se tiene un comité que centraliza todo incluyendo los temas de seguridad de la información, actualmente se tiene un borrador con el inventario de activos y sus responsables pero no ha sido aprobado. No se encuentran definidas las responsabilidades para la gestión del riesgo de SI y la aceptación de riesgos residuales, tampoco están documentados los niveles de autorización, ni se cuenta con un presupuesto formalmente asignado a las actividades de SGSI, el que existe es el general y de allí salen recursos pero no hay un formal para SI.	20	Ajustar el borrador tanto del Manual de Sistema de Gestión de la Seguridad de la Información y el de inventario de Activos, subsanando las brechas encontradas.

Cuadro 6. (Continuación)

			Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (PHVA) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia							
COMPONENTE	ID	CARGO	ÍTEM	DESCRIPCIÓN	PRUEBA	MSPI	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO PHVA	RECOMENDACIÓN
PLANIFICACIÓN	P.5	Responsable SI	Inventario de activos	Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	Solicite el inventario de activos de información, revisado y aprobado por la alta Dirección y revise: 1) Ultima vez que se actualizó 2) Que señale bajo algún criterio la importancia del activo 3) Que señale el propietario del activo Indague quien(es) el(los) encargado(s) de actualizar y revisar el inventario de activos y cada cuanto se realiza esta revisión. De acuerdo a NIST se deben considerar como activos el personal, dispositivos, sistemas e instalaciones físicas que permiten a la entidad cumplir con su misión y objetivos, dada su importancia y riesgos estratégicos. Tenga en cuenta para la calificación: 1) Si Se identifican en forma general los activos de información de la Entidad, están en 40. 2) Si se cuenta con un inventario de activos de información física y lógica de toda la entidad, documentado y firmado por la alta dirección, están en 60. 3) Si se revisa y monitorean periódicamente los activos de información de la entidad, están en 80.	componente planificación		Ambos documentos son borradores, por tanto no se encuentran aprobados	40	0
	P.6	Responsable SI	Identificación y valoración de riesgos	Metodología de análisis y valoración de riesgos e informe de análisis de riesgos	1) Solicite a la entidad la metodología y criterios de riesgo de seguridad, aprobado por la alta Dirección que incluya: 1. Criterios de Aceptación de Riesgos o tolerancia al riesgo que han sido informados por la alta Dirección. 2. Criterios para realizar evaluaciones de riesgos. 2) Solicite los resultados de las evaluaciones de riesgos y establezca: a. Cuantas evaluaciones repetidas de riesgos se han realizado y que sus resultados consistentes, válidos y comparables. b. Que se hayan identificado los riesgos asociados con la pérdida de la confidencialidad, de integridad y de disponibilidad de la información dentro del alcance. c. Que se hayan identificado los dueños de los riesgos. d. Que se hayan analizado los riesgos es decir: - Evaluado las consecuencias (impacto) potenciales si se materializan los riesgos identificados - Evaluado la probabilidad realista de que ocurran los riesgos identificados - Determinado los niveles de riesgo. e. Que se hayan evaluado los riesgos es decir: - Comparado los resultados del análisis de riesgos con los criterios definidos - Priorizado los riesgos analizados para el tratamiento de riesgos.	componente planificación	ESDESDIGGS02 Guía políticas para la administración del riesgo	Esta metodología no contempla los riesgo de seguridad de la información	20	
	P.7	Responsable SI	Tratamiento de riesgos de seguridad de la información	Los riesgos deben ser tratados para mitigarlos y llevarlos a niveles tolerables por la Entidad	1) Solicite el plan de tratamiento de riesgos y la declaración de aplicabilidad verifique que: a. Se seleccionaron opciones apropiadas para tratar los riesgos, teniendo en cuenta los resultados de la evaluación de riesgos. b. Se determinaron todos los controles necesarios para implementar las opciones escogidas para el tratamiento de riesgos. c. Compare los controles determinados en el plan de tratamiento con los del Anexo A y verifique que no se han omitidos controles, si estos han sido omitidos se debe reflejar en la declaración de aplicabilidad. d. Revise la Declaración de Aplicabilidad que tenga los controles necesarios y la justificación de las exclusiones, ya sea que se implementen o no y la justificación para las exclusiones de los controles del Anexo A, y que haya sido revisado y aprobado por la alta Dirección. e. Revise que el plan de tratamiento de riesgos haya sido revisado y aprobado por la alta Dirección. f. Revise que exista una aceptación de los riesgos residuales por parte de los dueños de los riesgos.	Modelo de Seguridad y Privacidad de la Información, componente planificación	ESDESDIGGS02 Guía políticas para la administración del riesgo	Validar	20	

Cuadro 6. (Continuación)

			Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (PHVA) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia							
COMPONENTE	ID	CARGO	ÍTEM	DESCRIPCIÓN	PRUEBA	MSPI	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO PHVA	RECOMENDACIÓN
PLANIFICACIÓN	P.7	Responsable SI	Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la Entidad, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	Entreviste a los líderes de los procesos y pregúnteles que saben sobre la seguridad de la información, cuáles son sus responsabilidades y como aplican la seguridad de la información en su diario trabajo. Pregunte como se asegura que los funcionarios, Directores, Gerentes y contratistas tomen conciencia en seguridad de la información, alineado con las responsabilidades, políticas y procedimientos existentes en la Entidad. Solicite el documento con el plan de comunicación, sensibilización y capacitación, con los respectivos soportes, revisado y aprobado por la alta Dirección. Verifique que se han tenido en cuenta buenas prácticas como: a) Desarrollar campañas, elaborar folletos y boletines. b) Los planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, están aprobados y documentados, por la alta Dirección c) Verifique que nuevos empleados y contratistas son objeto de sensibilización en SI. d) Indague cada cuanto o con qué criterios se actualizan los programas de toma de conciencia. e) Verifique que en las evidencias se puede establecer los asistentes al programa y el tema impartido. f) Incluir en los temas de toma de conciencia los procedimientos básicos de seguridad de la información (tales como el reporte de incidentes de seguridad de la información) y los controles de línea base (tales como la seguridad de las contraseñas, los controles del software malicioso, y los escritorios limpios). g) De acuerdo a NIST verifique que los funcionarios con roles privilegiados entienden sus responsabilidades y roles. Para la calificación tenga en cuenta que: Si Los funcionarios de la Entidad no tienen conciencia de la seguridad y privacidad de la información. Diseñar programas para la conciencia y comunicación, de las políticas de seguridad y privacidad de la información, están en 20. Si se observa en los funcionarios una conciencia de seguridad y privacidad de la información y los planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, deben estar aprobados y documentados, por la alta Dirección, están en 40. Si se han ejecutado los planes de toma de conciencia, comunicación y divulgación, de las políticas de seguridad y privacidad de la información, aprobados por la alta Dirección, están en 60.	componente planificación			0	
	P.8	Responsable de Tics	Plan y Estrategia de transición de IPv4 a IPv6	Las razones de que se requiera el cambio del protocolo de V4 a V6, se resumen a continuación: 1) Debido al aumento de la utilización de las redes de telecomunicaciones las direcciones de internet que permiten establecer conexiones para cada elementos conectado a la red, conocidas como direcciones IP (Internet Protocolo Versión 4), han entrado en una fase de agotamiento. 2) Mejora de la seguridad de la red en virtud de la arquitectura del nuevo protocolo y su servicio. En esta etapa se requiere hacer un diagnóstico que ayude a definir el plan y la estrategia para la transición entre los dos protocolos.	Verifique: 1) El Inventario de TI (Hardware, software) levantado 2) El análisis de la infraestructura actual de red de comunicaciones, recomendaciones para adquisición de elementos de comunicaciones, cómputo y almacenamiento, compatibles con el protocolo IPv6 3) El Protocolo de pruebas de validación de aplicativos, comunicaciones y bases de datos, el plan de seguridad y coexistencia de los protocolos. Plan de manejo de excepciones e informe de preparación de los sistemas de comunicaciones, bases de datos y aplicaciones. 4) El Plan de trabajo para la transición de los servicios tecnológicos de la Entidad de IPv4 a IPv6 5) La validación de estado actual de los sistemas de información y comunicaciones y la interfaz entre ellos y revisión de los RFC correspondientes. 6) La identificación de esquemas de seguridad de la información y seguridad de los sistemas de comunicaciones 7) Plan de capacitación en IPv6 a los funcionarios de las Áreas de TI de las Entidades y plan de sensibilización al total de funcionarios de las Entidades.	componente planificación	No se tiene	no se tiene	0	
PROMEDIO									**18**	**12**

Cuadro 6. (Continuación)

			Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (PHVA) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia							
COMPONENTE	ID	CARGO	ÍTEM	DESCRIPCIÓN	PRUEBA	MSPI	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO PHVA	RECOMENDACIÓN
IMPLEMENTACIÓN	I.1	Responsable SI	Planificación y control operacional	Estrategia que se debe ejecutar con las actividades para lograr la implementación y puesta en marcha del MSPI de la entidad.	Solicite y evalué el documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	componente implementación	no se tiene		0	
	I.2	n/a	Implementación de controles	Grado de implementación de controles del Anexo A de la ISO 27001	N/A	componente implementación		N/A	0	N/A
	I.3	Responsable SI	Implementación del plan de tratamiento de riesgos	Porcentaje de avance en la ejecución de los planes de tratamiento	Verifique los compromisos de avance en el plan de tratamiento de riesgos y el grado de cumplimiento de los mismos y genere un dato con el porcentaje de avance.	componente implementación	no se tiene		0	
	I.4	Responsable de Tics	Implementación del plan de estrategia de transición de IPv4 a IPv6	Porcentaje de avance en la ejecución de la de estrategia de transición de IPv4 a IPv6	Verifique: 1) De acuerdo al informe de plan detallado de implementación del nuevo protocolo la Habilitación direccionamiento IPv6 para cada uno de los componentes de hardware y software. 2) Solicite el documento con todas las configuraciones del nuevo protocolo realizadas y revise: a. La Configuración de servicios de DNS, DHCP, Seguridad, VPN, servicios WEB, b. La Configuración del protocolo IPv6 en Aplicativos, Sistemas de Comunicaciones, Sistemas de Almacenamiento. 3) La activación de políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones que posea cada entidad de acuerdo con los RFC de seguridad en IPv6. 4) La forma como se realizó la coordinación con el (los) proveedor (es) de servicios de Internet para lograr la conectividad integral en IPv6 hacia el exterior. 5) El Informe de resultados de las pruebas realizadas a nivel de comunicaciones, de aplicaciones y sistemas de almacenamiento.	componente implementación	no se tiene		0	
	I.5	Responsable SI	Indicadores de gestión del MSPI	Indicadores de gestión del MSPI definidos	Solicite los Indicadores de gestión del MSPI definidos, revisados y aprobados por la alta Dirección.	componente implementación	No se tiene		0	
PROMEDIO									**0**	**0**
EVALUACIÓN DE DESEMPEÑO	E.1	Responsable SI	Plan de seguimiento, evaluación y análisis del MSPI	Plan para evaluar el desempeño y eficacia del MSPI a través de instrumentos que permita determinar la efectividad de la implantación del MSPI.	Solicite y evalué el documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección.	componente evaluación del desempeño	no se tiene		0	
	E.2	Control Interno	Auditoría Interna	Plan de auditoría interna	Documento con el plan de auditorías internas y resultados, de acuerdo a lo establecido en el plan de auditorías, revisado y aprobado por la alta Dirección.	componente evaluación del desempeño	no se tiene	No se evidencia Auditoria enfocadas a Seguridad de la Información.	0	
	E.3	Responsable SI	Evaluación del plan de tratamiento de riesgos	Evaluación y seguimiento a los compromisos establecidos para ejecutar el plan de tratamiento de riesgos.	Resultado del seguimiento, evaluación y análisis del plan de tratamiento de riesgos, revisado y aprobado por la alta Dirección.	componente evaluación del desempeño	no se tiene		0	
PROMEDIO									**0**	**0**
MEJORA CONTINUA	M.1	Responsable SI	Plan de seguimiento, evaluación y análisis del MSPI	Resultados consolidados del componente evaluación de desempeño	Solicite y evalué el documento con el plan de seguimiento, evaluación y análisis para el MSPI, revisado y aprobado por la alta Dirección.	componente mejora continua	No se tiene		0	
	M.2	Control Interno	Auditoría Interna	Comunicación de los resultados y plan para subsanar los hallazgos y oportunidades de mejora.	Solicite el documento con el consolidado de las auditorías realizadas de acuerdo con el plan de auditorías, revisado y aprobado por la alta dirección y verifique como se asegura que los hallazgos, brechas, debilidades y oportunidades de mejora se subsanen, para asegurar la mejora continua. **Tenga en cuenta para la calificación que:** 1) Elaboración de planes de mejora es 60 2) Se implementan las acciones correctivas y planes de mejora es 80	componente mejora continua	no se tiene	0	0	0
PROMEDIO									**0**	**0**

Fuente: Instrumento de evaluación del MINTIC

Cuadro 7. Nivel de madurez modelo de seguridad y privacidad de la información

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Nivel de madurez MSPI) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia														vive digital para la gente
ID REQUISITO	**CARGO**	**REQUISITO**	**HOJA**	**ELEMENTO**	**CALIFICACIÓN OBTENIDA**	**NIVEL 1 INICIAL**	**CUMPLIMIENTO NIVEL INICIAL**	**NIVEL 2 GESTIONADO**	**CUMPLIMIENTO NIVEL GESTIONADO**	**NIVEL 3 DEFINIDO**	**CUMPLIMIENTO NIVEL DEFINIDO**	**NIVEL 4 GESTIONADO CUANTITATIVAMENTE**	**CUMPLIMIENTO NIVEL 4 GESTIONADO CUANTITATIVAMENTE**	**NIVEL 5 OPTIMIZADO**	**CUMPLIMIENTO NIVEL 5 OPTIMIZADO**
R1	n/a	1) Si Se identifican en forma general los activos de información de la Entidad, están en 40. 2) Si se cuenta con un inventario de activos de información física y lógica de toda la entidad, documentado y firmado por la alta dirección, están en 60. 3) Si se revisa y monitorean periódicamente los activos de información de la entidad, están en 80.	Administrativas	AD.4.1.1	40	40	CUMPLE	60	MENOR	60	MENOR	80	MENOR	100	MENOR
R2	n/a	Se clasifican los activos de información lógicos y físicos de la Entidad.	Administrativas	AD.4.2.1	20	20	CUMPLE	40	MENOR	60	MENOR	80	MENOR	100	MENOR
R3	n/a	1. Si Los funcionarios de la Entidad no tienen conciencia de la seguridad y privacidad de la información y se han diseñado programas para los funcionarios de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, están en 20. 2. Si se observa en los funcionarios una conciencia de seguridad y privacidad de la información y los planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, están aprobados y documentados, por la alta Dirección, están en 40. 3. Si se han ejecutado los planes de toma de conciencia, comunicación y divulgación, de las políticas de seguridad y privacidad de la información, aprobados por la alta Dirección, están en 60.	Administrativas	AD.3.2.2	20	20	CUMPLE	40	MENOR	60	MENOR	80	MENOR	100	MENOR

Cuadro 7. (Continuación)

Instrumento de identificación de la línea base de seguridad
hoja levantamiento de información
(Nivel de madurez MSPI)
Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia

ID REQUISITO	CARGO	REQUISITO	HOJA	ELEMENTO	CALIFICACIÓN OBTENIDA	NIVEL 1 INICIAL	CUMPLIMIENTO NIVEL INICIAL	NIVEL 2 GESTIONADO	CUMPLIMIENTO NIVEL GESTIONADO	NIVEL 3 DEFINIDO	CUMPLIMIENTO NIVEL DEFINIDO	NIVEL 4 GESTIONADO CUANTITATIVAMENTE	CUMPLIMIENTO NIVEL 4 GESTIONADO CUANTITATIVAMENTE	NIVEL 5 OPTIMIZADO	CUMPLIMIENTO NIVEL 5 OPTIMIZADO
R4		Existe la necesidad de implementar el Modelo de Seguridad y Privacidad de la Información, para definir políticas, procesos y procedimientos claros para dar una respuesta proactiva a las amenazas que se presenten en la Entidad.	PHVA	P.1	20	20	CUMPLE	40	MENOR	60	MENOR	80	MENOR	100	MENOR
			Administrativas	AD.1.1	40	20	MAYOR	40	CUMPLE	60	MENOR	80	MENOR	100	MENOR
			PHVA	P.4	20	20	CUMPLE	40	MENOR	60	MENOR	80	MENOR	100	MENOR
R5	Responsable de SI	1. Si se tratan temas de seguridad y privacidad de la información en los comités del modelo integrado de gestión, coloque 20 2.Los temas de seguridad de la información se tratan en los comités directivos interdisciplinarios de la Entidad, con regularidad, coloque 40	Madurez	R5	0	20	MENOR	40	MENOR	60	MENOR	80	MENOR	100	MENOR
R6	n/a	1. Si se empiezan a definir las políticas de seguridad y privacidad de la información basada en el Modelo de Seguridad y Privacidad de la Información, están en 20. 2. Si se revisan y se aprueban las políticas de seguridad y privacidad de la información, están en 40. 3. Si se divulgan las políticas de seguridad y privacidad de la información, están en 60.	Administrativas	AD.1.1	40	20	MAYOR	40	CUMPLE	60	MENOR	80	MENOR	100	MENOR
R7	n/a	Establecer y documentar el alcance, limites, política, procedimientos, roles y responsabilidades y del Modelo de Seguridad y Privacidad de la Información.	PHVA	P.1	20	60	MENOR	60	MENOR	60	MENOR	80	MENOR	100	MENOR
R8	n/a	Determinar el impacto que generan los eventos que atenten contra la integridad, disponibilidad y confidencialidad de la información de la Entidad.	Técnicas	T.7.1.4	20	20	CUMPLE	40	MENOR	60	MENOR	60	MENOR	80	MENOR
LIMITE DE MADUREZ INICIAL					240	260	MENOR	440	MENOR	600	MENOR	780	MENOR	980	MENOR

Cuadro 7. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (nivel de madurez MSPI) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia														vive digital para la gente
ID REQUISITO	**CARGO**	**REQUISITO**	**HOJA**	**ELEMENTO**	**CALIFICACIÓN OBTENIDA**	**NIVEL 1 INICIAL**	**CUMPLIMIENTO NIVEL INICIAL**	**NIVEL 2 GESTIONADO**	**CUMPLIMIENTO NIVEL GESTIONADO**	**NIVEL 3 DEFINIDO**	**CUMPLIMIENTO NIVEL DEFINIDO**	**NIVEL 4 GESTIONADO CUANTITATIVAMENTE**	**CUMPLIMIENTO NIVEL 4 GESTIONADO CUANTITATIVAMENTE**	**NIVEL 5 OPTIMIZADO**	**CUMPLIMIENTO NIVEL 5 OPTIMIZADO**
R24	n/a	Responsabilidades del usuario frente al control de accesos	Técnicas	T.1.2.6	0	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R25	n/a	Seguridad física y ambiental en áreas seguras	Técnicas	T.1.3.1	0	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R26	n/a	Seguridad física y ambiental de los equipos	Técnicas	T.3.2	0	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R27	n/a	Responsabilidades y procedimientos de operación	Técnicas	T.4.1	0	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R28	n/a	Seguridad en la operativa, control del software en explotación	Técnicas	T.4.5	0	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R29	n/a	Gestión de la seguridad en las redes.	Técnicas	T.5.1	0	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R30	n/a	Intercambio de información con partes externas	Técnicas	T.5.2	0	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R31	n/a	Adquisición, desarrollo y mantenimiento de los sistemas de información, requisitos de seguridad de los sistemas de información.	Técnicas	T.6.1	0	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R32	n/a	Adquisición, desarrollo y mantenimiento de los sistemas de información, seguridad en los procesos de desarrollo y soporte.	Técnicas	T.6.2	2	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R33	n/a	Adquisición, desarrollo y mantenimiento de los sistemas de información, datos de prueba.	Técnicas	T.6.3	0	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R34	n/a	Gestión de incidentes en la seguridad de la información, notificación de los eventos de seguridad de la información.	Técnicas	T.7.1.2	20	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R35	n/a	Gestión de incidentes en la seguridad de la información, notificación de puntos débiles de la seguridad.	Técnicas	T.7.1.3	20	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R36	n/a	Gestión de incidentes en la seguridad de la información, recopilación de evidencias.	Técnicas	T.7.1.7	20	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R37	n/a	Implantación de la continuidad de la seguridad de la información.	Administrativas	AD.5.1.2	0	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R38	Responsable de compras y adquisiciones	Seguridad de la información en las relaciones con suministradores.	Administrativas	AD.7.1	0	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR

Cuadro 7. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (nivel de madurez MSPI) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia													vive digital para la gente	
ID REQUISITO	**CARGO**	**REQUISITO**	**HOJA**	**ELEMENTO**	**CALIFICACIÓN OBTENIDA**	**NIVEL 1 INICIAL**	**CUMPLIMIENTO NIVEL INICIAL**	**NIVEL 2 GESTIONADO**	**CUMPLIMIENTO NIVEL GESTIONADO**	**NIVEL 3 DEFINIDO**	**CUMPLIMIENTO NIVEL DEFINIDO**	**NIVEL 4 GESTIONADO CUANTITATIVAMENTE**	**CUMPLIMIENTO NIVEL 4 GESTIONADO CUANTITATIVAMENTE**	**NIVEL 5 OPTIMIZADO**	**CUMPLIMIENTO NIVEL 5 OPTIMIZADO**
R39	Responsable de compras y adquisiciones	Gestión de la prestación del servicio por suministradores.	Administrativas	AD.7.2	20	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
R40	n/a	Se implementa el plan de tratamiento de riesgos y las medidas necesarias para mitigar la materialización de las amenazas.	PHVA	P.8	20	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR	100	MENOR
LIMITE DE MADUREZ DEFINIDO					102	0		0		660	MENOR	880	MENOR	1100	MENOR
R41	n/a	Se utilizan indicadores de cumplimiento para establecer si las políticas de seguridad y privacidad de la información y las clausulas establecidas por la organización en los contratos de trabajo, son acatadas correctamente. Se deben generar informes del desempeño de la operación del MSPI, con la medición de los indicadores de gestión definidos.	PHVA	I.5	0	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
			PHVA	E.1	0	N/A	N/A	N/A	N/A	N/A	N/A	40	MENOR	60	MENOR
			PHVA	E.2	0	N/A	N/A	N/A	N/A	N/A	N/A	40	MENOR	60	MENOR
			PHVA	E.3	0	N/A	N/A	N/A	N/A	N/A	N/A	40	MENOR	60	MENOR
			PHVA	M.1	0	N/A	N/A	N/A	N/A	N/A	N/A	40	MENOR	60	MENOR
R42	n/a	Se realizan pruebas de manera sistemática a los controles, para determinar si están funcionando de manera adecuada. Se deben generar informes del desempeño de la operación del MSPI, con la revisión y verificación continua de los controles implementados. También se generan informes de auditorías de acuerdo a lo establecido en el plan de auditorías de la entidad. Se realizan pruebas de efectividad en la Entidad, para detectar vulnerabilidades (físicas, lógicas y humanas) y accesos no autorizados a activos de información críticos.	Administrativas	AD.6.2	0	N/A	N/A	N/A	N/A	N/A	N/A	40	MENOR	60	MENOR
R43	n/a	1) Se realizan pruebas y ventanas de mantenimiento (simulacro), para determinar la efectividad de los planes de respuesta de incidentes, es 60. 2) Si La Entidad aprende continuamente sobre los incidentes de seguridad presentados, es 80.	Técnicas	T.7.1.6	20	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR

Cuadro 7. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Nivel de madurez MSPI) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia														vive digital para la gente
ID REQUISITO	CARGO	REQUISITO	HOJA	ELEMENTO	CALIFICACIÓN OBTENIDA	NIVEL 1 INICIAL	CUMPLIMIENTO NIVEL INICIAL	NIVEL 2 GESTIONADO	CUMPLIMIENTO NIVEL GESTIONADO	NIVEL 3 DEFINIDO	CUMPLIMIENTO NIVEL DEFINIDO	NIVEL 4 GESTIONADO CUANTITATIVAMENTE	CUMPLIMIENTO NIVEL 4 GESTIONADO CUANTITATIVAMENTE	NIVEL 5 OPTIMIZADO	CUMPLIMIENTO NIVEL 5 OPTIMIZADO
R44	n/a	Se realizan pruebas a las aplicaciones o software desarrollado "in house" para determinar que cumplen con los requisitos de seguridad y privacidad de la información	Técnicas	T.6.2.8	0	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
R45	n/a	Registro de actividades en seguridad (bitácora operativa).	Técnicas	T.4.4.1	0	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
R46	n/a	1) Elaboración de planes de mejora es 60 2) Se implementan las acciones correctivas y planes de mejora es 80	PHVA	M.2	0	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
R47	n/a	1) Si los planes de respuesta a incidentes incluyen algunas áreas de la entidad y si se evalúa la efectividad los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro es 60 2) Se incluyen todas las áreas de la Entidad, en los planes de respuesta de incidentes es 80	Técnicas	T.7.1.5	20	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
R48	n/a	Gestión de acceso de usuario.	Técnicas	T.1.2	7	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
R49	n/a	Control de acceso a sistemas y aplicaciones	Técnicas	T.1.4	8	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
R50	n/a	Controles Criptográficos	Técnicas	T.2.1	0	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
R51	n/a	Consideraciones de las auditorías de los sistemas de información.	Técnicas	T.4.4	0	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
R52	n/a	Seguridad en la operativa, registro de actividad y supervisión.	Técnicas	T.4.7	0	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
R53	n/a	Cumplimiento de los requisitos legales y contractuales.	Administrativas	AD.6.1	55	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
R44	n/a	Se realizan pruebas a las aplicaciones o software desarrollado "in house" para determinar que cumplen con los requisitos de seguridad y privacidad de la información	Técnicas	T.6.2.8	0	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
R45	n/a	Registro de actividades en seguridad (bitácora operativa).	Técnicas	T.4.4.1	0	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
R46	n/a	1) Elaboración de planes de mejora es 60 2) Se implementan las acciones correctivas y planes de mejora es 80	PHVA	M.2	0	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR

Cuadro 7. (Continuación)

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento de identificación de la línea base de seguridad hoja levantamiento de información (Nivel de madurez MSPI) Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia														vive digital para la gente
ID REQUISITO	**CARGO**	**REQUISITO**	**HOJA**	**ELEMENTO**	**CALIFICACIÓN OBTENIDA**	**NIVEL 1 INICIAL**	**CUMPLIMIENTO NIVEL INICIAL**	**NIVEL 2 GESTIONADO**	**CUMPLIMIENTO NIVEL GESTIONADO**	**NIVEL 3 DEFINIDO**	**CUMPLIMIENTO NIVEL DEFINIDO**	**NIVEL 4 GESTIONADO CUANTITATIVAMENTE**	**CUMPLIMIENTO NIVEL 4 GESTIONADO CUANTITATIVAMENTE**	**NIVEL 5 OPTIMIZADO**	**CUMPLIMIENTO NIVEL 5 OPTIMIZADO**
R47	n/a	1) Si los planes de respuesta a incidentes incluyen algunas áreas de la entidad y si se evalúa la efectividad los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro es 60 2) Se incluyen todas las áreas de la Entidad, en los planes de respuesta de incidentes es 80	Técnicas	T.7.1.5	20	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
R48	n/a	Gestión de acceso de usuario.	Técnicas	T.1.2	7	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
R49	n/a	Control de acceso a sistemas y aplicaciones	Técnicas	T.1.4	8	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
R50	n/a	Controles Criptográficos	Técnicas	T.2.1	0	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
R51	n/a	Consideraciones de las auditorías de los sistemas de información.	Técnicas	T.4.4	0	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
R52	n/a	Seguridad en la operativa, registro de actividad y supervisión.	Técnicas	T.4.7	0	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
R53	n/a	Cumplimiento de los requisitos legales y contractuales.	Administrativas	AD.6.1	55	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR	80	MENOR
LIMITE DE MADUREZ GESTIONADO CUANTITATIVAMENTE					110	0		0		0		660	MENOR	880	MENOR
R55	n/a	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Administrativas	AD.5.1.3	0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	60	MENOR
LIMITE DE MADUREZ OPTIMIZADO					330									1660	MENOR
Fuente: Instrumento de evaluación del MINTIC															

ANEXO B. Política General y Específicas Seguridad de la Información FPS

POLITICAS GENERAL Y ESPECÍFICAS DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

FONDO DE PASIVO SOCIAL
FERROCARRILES NACIONALES DE COLOMBIA

Fecha de Vigencia:

CONTROL DE DOCUMENTOS			
Elaborado por: Roselys Silva Cuadrado y Henry Jara Velandia	**Cargo:** Profesional y Apoyo	**Fecha: Marzo/01/2016**	**Firma:**
Revisado Técnicamente en OPS:	**Cargo:**	**Fecha:**	**Firma:**
Aprobado Mediante Acta No : **Acto Administrativo:** **Fecha:**			

CONTROL DE CAMBIOS:			
Versión	**Fecha y acto administrativo de aprobación**	**Cambio**	**Nombre del solicitante**
1.0			Mauricio Villaneda Jiménez

CAPITULO I POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

EL DIRECTOR GENERAL DEL FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA

En ejercicio de sus facultades legales y estatutarias, en especial de las que le confiere el artículo 10 del decreto 1591 de 1989; el Decreto 3968 de 2008; las leyes 962 de 2005; 1474 de 2011; 1437 de 2011; 1450 de 2011, el Decreto 019 de 2012, en especial el Decreto 2693 de 2012 y demás facultades constitucionales y legales, y

CONSIDERANDO:

POLÍTICA DE SEGURIDAD 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, la seguridad de la información busca la disminución en el impacto generado sobre sus activos, 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.

De acuerdo con lo anterior, esta política aplica a la entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinados por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.

- Cumplir con los principios de seguridad de la información.

- Cumplir con los principios de la función administrativa.

- Mantener la confianza de sus usuarios y funcionarios.

- Apoyar la innovación tecnológica.

- Proteger los activos tecnológicos.

- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros y usuarios del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA.

- Garantizar la continuidad de la entidad frente a incidentes.

- El FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA ha decidido implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

CAPITULO II DISPOSICIONES GENERALES

ARTÍCULO PRIMERO OBJETO

La presente resolución tiene como objeto la adopción de la política de seguridad de la información del Fondo Pasivos Social Ferrocarriles Nacionales de Colombia, así como definir lineamiento frente a su uso y manejo.

ARTÍCULO SEGUNDO OBJETIVOS DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA

Objetivo general Diseñar un plan de seguridad y privacidad de la información mediante la aplicación de la estrategia de gobierno en línea y la norma ISO 27001:2013 con el fin de implementar un sistema de gestión de seguridad de la información dentro del Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia durante la vigencia 2017.

Estén autorizados en la necesidad legítima para la realización de funciones propias de la entidad, que estén protegidos contra modificaciones no planeadas o realizadas con o sin intención y a sus activos asociados estén disponibles cuando se le requieran contribuyendo a la continuidad en la prestación de los servicios ofrecidos a la ciudadanía.

Objetivos específicos 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.

- Establecer una política de seguridad y privacidad de la información donde se evidencie el compromiso de la alta dirección frente al aseguramiento la seguridad asociada al recurso humano, físico y ambiental y a la administración del riesgo de seguridad de la información.

- Realizar capacitación, sensibilización y comunicación de la seguridad y privacidad de la información, asegurando que cada uno cumpla con sus roles y responsabilidades de seguridad y privacidad de la información dentro de la entidad.

- Revisar periódicamente el cumplimiento de los requisitos legales que en materia de seguridad y privacidad de la información apliquen a la entidad.

ARTÍCULO TERCERO ALCANCE/APLICABILIDAD

Esta política aplica a toda la entidad, sus funcionarios, terceros, proveedores del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA y la ciudadanía en general.

ARTÍCULO CUARTO ROLES Y RESPONSABILIDADES

Encargado de la seguridad de la información Desarrollar las políticas de seguridad de la información al interior de la entidad, liderar, coordinar su implementación de las políticas de seguridad de la información, con la participación activa de las dependencias de la Entidad y velar por su correcta aplicación.

- Revisar la efectividad de los controles establecidos y coordinar la implementación de controles específicos para nuevos sistemas de información o servicios informáticos.

- Impulsar la cultura de seguridad de la información dentro de la entidad.

- Reportar y atender a los requerimientos de seguridad antes los equipos de respuestas a incidentes (CSIRT PONAL, Ministerios, entre otros) que lo requieran.

- Constituir un programa periódico (por lo menos una vez al año) para la revisión de vulnerabilidades de la plataforma tecnológica de la Entidad y coordinar los respectivos aseguramientos o acciones conforme los resultados de las mencionadas pruebas.

- Mantener un inventario de los activos de información en la entidad y clasificarlos según sea su tipo con la con la participación activa de las dependencias de la Entidad.

- Monitorear el avance general de la gestión y tratamiento de riesgos que permita e control de las amenazas.

- Identificar las necesidades y recursos necesarios (tecnológicos, humanos, de capacitación, financieros, etc.) para el mantenimiento de la infraestructura de seguridad de la información.

- Realizar seguimiento al SGSI.

- Actuar como un asesor en seguridad de la información para la Entidad.

- Hacer seguimiento al comportamiento de los indicadores de gestión de la seguridad de la información que adopte el Comité de desarrollo administrativo.

- Hacer la evaluación del desempeño del SGSI.

- Presentar y reportar al Comité de desarrollo administrativo el estado y monitoreo de los incidentes de seguridad de la información, los resultados de las auditorias periódicas y la revisión del SGSI.

- Establecer puntos de enlaces con encargados de seguridad de la información de otras entidades y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.

- Revisar periódicamente los niveles de acceso a los sistemas de información.

- Determinar los requerimientos de copias de respaldo para la información de la entidad.

- Tomar las acciones adecuadas en caso de violaciones de seguridad.

- Verificar periódicamente la integridad y coherencia de la información producto de los procesos.

- Las demás que le asigne el director general

Propietario de la información son los dueños o encargados 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.

Entre las responsabilidades de los propietarios de información se tienen:

- Asignar los niveles iníciales de clasificación de información.

- Revisión y actualización periódica (por lo menos una vez al año) de la clasificación de la información con el propósito de verificar que cumpla con los requerimientos de la entidad y leyes vigentes.

- Determinar los criterios y niveles de acceso a la información.

- Definir los controles de seguridad para la información que tiene a su cargo.

Custodio de la información En el fondo los encargados de la custodia de la información son los procesos de Gestión Documental y Gestión de TIC 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, contratistas, proveedores, entidades que con la debida autorización del propietario de la información, puede generar 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.

Los usuarios solo deben tener acceso a la información a la que están autorizados a consultar y procesar. Las autorizaciones que se otorguen limitaran su capacidad en los entornos informáticos de forma que no pueden realizar actividades diferentes a las autorizadas.

Las responsabilidades de los usuarios finales, es decir, aquellas personas que utilizan información del Fondo como parte de su trabajo diario están definidas a continuación:

- Mantener la confidencialidad de las contraseñas de aplicaciones y sistemas.

- Cumplir con los controles establecimientos en las políticas y procedimientos de seguridad de la información definidos por la entidad.

- Comunicar los incidentes relativos de la seguridad de información.

- Asegurarse de ingresar información adecuada a los sistemas.

- Adecuarse a las políticas y procedimientos de seguridad de la información definidos por la entidad.

- Utilizar la información solo o únicamente para los propósitos autorizados.

- Tomar las medidas adecuadas para evitar que la información se divulgue o use sin autorización.

ARTÍCULO QUINTO NIVEL DE CUMPLIMIENTO

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

A continuación se establecen las 21 Reglas de seguridad que soportan el SGSI del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA:

1. Definirá, Implementará, Operará y Mejorará de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de la entidad, y a los requerimientos regulatorios.

2. Definirá las responsabilidades frente a la seguridad de la información compartida, publicada y aceptadas por cada uno de los funcionarios, proveedores o terceros.

3. Protegerá la información generada, procesada o resguardada por los procesos, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

4. Definirá y Establecerá controles de acuerdo con la clasificación de la información de su propiedad o en custodia para proteger la información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto, accesos no autorizados, violaciones y perdida de integridad de la información.

5. Protegerá su información de las amenazas originadas por parte del personal.

6. Protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

7. Controlará la operación de sus procesos garantizando la seguridad de los recursos tecnológicos y las redes de datos.

8. Implementará control de acceso a la información, sistemas y recursos de red.

9. Garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

10. Garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

11. Garantizará la disponibilidad de sus procesos y la continuidad de su operación basada en el impacto que pueden generar los eventos.

12. Garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

13. Solo permitirá el uso de software autorizado y/o adquirido legalmente por la entidad.

14. Todos los funcionarios y/o contratistas, serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

15. Todos los funcionarios y/o contratistas, serán responsables de reportar los incidentes de seguridad, mal uso de los recursos y eventos sospechosos de los que tenga conocimiento.

16. Todos los funcionarios y/o contratistas, deberán acatar y dar cumplimiento a los lineamientos dispuestos en el manual de uso del Sistema de Gestión de Seguridad de la Información.

17. Todos los equipos de propiedad del Fondo deben contar con la fecha y hora exactas para que el registro de los archivos de auditoría sea el correcto.

18. Cualquier auditoría de seguridad a los sistemas del fondo debe estar debidamente autorizada y aprobada por el jefe de oficina asesora de Planeación y sistemas, con visto bueno del Director.

19. Las auditorías de seguridad de la información deben ser realizadas por personal preparado técnicamente, en caso de no existir, el personal asignado debe ser capacitado adecuadamente.

20. Las claves y contraseñas asignadas a cada funcionario son de carácter personal e intransferible, su uso debe ser de manera responsable, tener un buen manejo, efectuar cambios de manera periódica y por seguridad deben ser alfanumérica de mínimo 8 caracteres e incluir Mayúsculas y minúsculas; No se permite el préstamo de claves y contraseñas.

21. Cumplir con la política de buen uso y manejo de los equipos de cómputo, los servicios institucionales de correo electrónico e internet.

Esta política de seguridad deberá seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, desarrollo de nuevos servicios, nuevos lineamientos normativos o de ley, entre otros.

ARTÍCULO SEXTO REVISIÓN Y MONITOREO

La Política General de Seguridad y Privacidad de la Información será revisada o evaluada su cumplimiento semestralmente o cuando requiera modificaciones con el

objeto de mantenerla actualizada Este proceso será liderado por gestión TIC´S, y revisado por la oficina de planeación y sistemas y aprobado por el comité de desarrollo administrativo, considerando los siguientes aspectos:

- Condiciones contractuales, reguladora 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.

ARTÍCULO SEPTIMO DIFUSIÓN

El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia comunicará todas las políticas, procedimiento 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.

Serán publicados en la intranet y página web del fondo 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 de incorporar la aplicación y observancia de las Políticas de Seguridad y Privacidad de la Información, en el plan de capacitación institucional, junto con velar por la correcta inducción y re inducción de los funcionarios en materias de seguridad y privacidad de la información.

ARTÍCULO OCTAVO SANCIONES

A los funcionarios, contratistas, así como aquellos procesos externos que estén vinculados por contratos o acuerdos con terceros que infrinjan esta política; se les apicaran medidas correctivas que pueden ser desde acciones correctivas hasta acciones de orden disciplinario o penal, de acuerdo a las circunstancias si así lo ameritan y siempre sujetos a la aplicación de la normatividad de tipo disciplinario y penal vigente.

ARTÍCULO NOVENO VIGENCIAS

La presente resolución rige a partir de la fecha de su expedición.

COMUNICASE Y CUMPLASE:
JAIME LUIS LACOUTURE PEÑALOZA
Director General

CAPITULO III POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ARTÍCULO DECIMO POLÍTICA DE ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN

El FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA establecerá un esquema para la seguridad de la información que cuente con roles y responsabilidades definidas que consideren actividades como la operación gestión y administración de la seguridad de la información en la entidad.

A continuación se establecen las medidas de la política de estructura organizacional de seguridad de la información del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA:

- La Alta Dirección del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA debe definir y establecer las respectivas responsabilidades y roles relacionados con la seguridad de la información.

- La Alta Dirección debe revisar y aprobar las Políticas de Seguridad de la Información que han sido definidas en este documento.

- La Alta Dirección debe promover dentro de la entidad, una cultura de seguridad de la información de forma activa y permanente.

- La Alta Dirección debe facilitar la socialización de las Políticas de Seguridad de la información a todo el personal de la entidad.

- La Alta Dirección, debe asignar los recursos, la infraestructura y el personal que sea necesario para la gestión correcta de la seguridad de la información del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA.

- El Comité de Seguridad de la Información o el que haga sus veces, debe revisar, actualizar y presentar ante la alta dirección as Políticas de Seguridad de la Información, la metodología para la gestión del riesgo, la clasificación de la información, y demás temas relacionados.

- El Comité de Seguridad de la Información o el que haga sus veces, debe analizar los incidentes de seguridad que le sean escalados y realizar el debido proceso de contacto con las autoridades en caso de ser necesario.

- El Comité de Seguridad de la Información o el que haga sus veces, debe constatar que se cumplan las políticas de seguridad de la información mencionadas en este documento.

- La Oficina de Control Interno o la que haga sus veces, debe planificar y ejecutar las auditorías internas al Sistema de Gestión de Seguridad de la Información del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA con el fin de determinar si las políticas, procedimientos, controles y procesos establecidos están acordes con los requerimientos de la entidad en cuanto a institucionalidad, seguridad y regulaciones aplicables.

- La Oficina de Control Interno o la que haga sus veces, debe realizar revisiones parciales y totales de todos los procesos o áreas que hagan parte del alcance del Sistema de Gestión de Seguridad de la Información de la entidad, de manera que pueda de verificar la eficacia de las acciones preventivas y correctivas que se realicen.

- La Oficina de Control Interno o la que haga sus veces debe informar a las personas y áreas responsables cuando se encuentren hallazgos durante las auditorias.

- El proceso Gestión TIC´S debe asignar los roles, responsabilidades y funciones al personal que se requiera para la operación y administración del Sistema de Gestión de Seguridad de la Información, donde esto debe estar debidamente documentado y segregado.

ARTÍCULO DECIMO PRIMERO POLÍTICA PARA USO DE CONEXIONES REMOTAS

El FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA establecerá las circunstancias y requisitos bajo las cuales se permitirá el establecimiento de conexiones remotas a la plataforma tecnológica de la entidad; Del mismo modo, facilitará las herramientas necesarias para garantizar que dichas conexiones se realicen de forma segura.

A continuación se establecen las medidas de la política para uso de conexiones remotas del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA:

- El proceso Gestión TIC´S debe revisar y aprobar los métodos de conexión remota a la plataforma tecnológica de la entidad.

- El proceso Gestión TIC´S debe restringir las conexiones remotas; permitiendo únicamente que estas se realicen por personal autorizado y por lapso de tiempo previamente establecidos, de acuerdo con la labor a desempeñarse durante la conexión.

- El proceso Gestión TIC´S debe validar la efectividad de los controles aplicados sobre las conexiones remotas de forma permanente.

- La Oficina de Control Interno debe, dentro de su autonomía, realizar las respectivas auditorías sobre los controles implantados para las conexiones remotas de la entidad.

- Los usuarios que realicen conexión remota deben tener las aprobaciones requeridas para establecer dicha conexión y siempre deben respetar las condiciones de uso establecidas para las conexiones.

- Los usuarios únicamente deben establecer conexiones remotas en equipos identificados previamente, evitando en todo momento el uso de computadores públicos, cafés internet y demás similares.

ARTÍCULO DECIMO SEGUNDO POLÍTICA DE SEGURIDAD DEL PERSONAL

El FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA reconoce la importancia que tiene el recurso humano para el logro de los objetivos de la entidad, por tal razón y con el fin de contar con personal altamente calificado, garantizará que la vinculación de funcionarios se realizará bajo un proceso formal de selección, acorde con la legislación vigente.

A continuación se establecen las medidas de la política de seguridad del personal del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA:

- La Oficina Asesora Jurídica y el proceso Gestión de Talento Humano deben realizar las verificaciones que se requieran para confirmar la veracidad de la información que sea suministrada por el posible personal a ocupar un cargo en El FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA, antes de realizar cualquier vinculación con el mismo.

- La Oficina Asesora Jurídica y el proceso Gestión de Talento Humano deben garantizar que los funcionarios de la entidad firmen un Acuerdo y/o Cláusula de Confidencialidad así como un documento de Aceptación de Políticas de Seguridad de la Información; estos documentos deben ser adjuntos a los demás documentos relacionados con la vinculación del personal.

- Cada Supervisor de Contrato, jefe inmediato y/o similar debe constatar la existencia de Acuerdos y/o Cláusulas de Confidencialidad así como del documento de Aceptación de Políticas de Seguridad de la Información antes de dar cualquier acceso a la información del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA.

- El personal provisto por terceros para realizar labores en o para el FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA debe firmar un Acuerdo y/o Cláusula de Confidencialidad y el documento de Aceptación

de Políticas de Seguridad de la Información, antes de que se les facilite cualquier acceso a las instalaciones y a la plataforma tecnológica de la entidad.

ARTÍCULO DECIMO TERCERO POLÍTICA DE DESVINCULACIÓN, LICENCIAS, CAMBIO DE LABOR, VACACIONES DE PERSONAL Y CONTRATISTAS

El FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA, garantizara que su personal, y contratitas sea desvinculado o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura.

A continuación se establecen las medidas de la política de desvinculación, licencias, cambio de labor o vacaciones de personal y contratistas del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA:

- El proceso Gestión de Talento Humano debe realizar el proceso de desvinculación, licencias, cambio de labor, vacaciones de personal y contratistas de la entidad, realizando los procedimientos y controles establecidos para dicha finalidad.

- Cada Supervisor de Contrato, Jefe de Oficina o similar, debe monitorear y reportar de manera inmediata la desvinculación o cambio de labores de personal o contratistas de la entidad tanto al proceso Gestión de TIC´S quien realizará la modificación o inhabilitación de usuarios.

ARTÍCULO DECIMO CUARTO POLÍTICA DE USO DE MEDIOS DE ALMACENAMIENTO Y PERIFÉRICOS

El uso de medios de almacenamiento y periféricos en los recursos de la plataforma tecnológica del DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA será estipulado por el proceso Gestión de TIC´S considerando las labores que realice el personal y las necesidades respectivas.
A continuación se establecen las medidas de la política de uso de medios de almacenamiento y periféricos del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA:

- El proceso Gestión TIC´S en conjunto con el comité de Seguridad de la Información o el que haga sus veces, deben establecer las condiciones para el uso de medios de almacenamiento y periféricos dentro de la plataforma tecnológica del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA.

- El proceso Gestión TIC´S debe estipular y aplicar el proceso para la disposición segura de los medios de almacenamiento de la entidad cuando estos sean dados de baja o re-asignados a otro usuario.

ARTÍCULO DECIMO QUINTO: POLÍTICA DE ACCESO A REDES Y RECURSOS DE RED

El proceso Gestión TIC´S, como responsables de las redes de datos y los recursos de red del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA, debe buscar que las redes sean protegidas de manera adecuada contra accesos no autorizados a través de mecanismos de control de acceso.

A continuación se establecen las medidas de la política de acceso a redes y recursos de red del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA:

- El proceso Gestión TIC´S debe establecer un procedimiento y unos debidos controles para proteger el acceso tanto a las redes de datos como a los recursos de red de la entidad.

- El proceso Gestión TIC´S bajo la supervisión de los líderes de procesos, debe autorizar la creación y/o modificación de las cuentas de acceso a las redes o recursos de red del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA.

- El proceso Gestión TIC´S debe verificar de forma periódica todos los controles de acceso a los recursos de red y servicios de la plataforma de la entidad.

• Los equipos que se conecten o deseen conectarse a las redes de datos de la entidad, deben cumplir con los requisitos o controles dispuestos para ello, y solo podrán realizar las tareas para las que fueron autorizados.

ARTÍCULO DECIMO SEXTO POLÍTICA DE CONTROL DE ACCESO

El proceso Gestión TIC´S debe controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática.

A continuación se establecen las medidas de la política de control de acceso del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA:

• Las claves y contraseñas asignadas a cada funcionario son de carácter personal e intransferible, su uso debe ser de manera responsable, tener un buen manejo, efectuar cambios de manera periódica y por seguridad deben ser alfanumérica de mínimo 8 caracteres e incluir mayúsculas y minúsculas; No se permite el préstamo de claves y contraseñas.

• Los funcionarios al abandonar temporalmente su puesto de trabajo deben bloquear sus sesiones y al finalizar la jornada laboral o cuando exista ausencia temporal que supere dos (2) horas deberán a pagar sus equipos o estaciones de trabajo.

• El oficial de seguridad de la información deber establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información, los cuales debe comprender todas las fases del ciclo de vida del acceso del usuario, desde el registro inicial de los usuarios nuevos hasta la cancelación final del registro de usuarios que ya no requieren acceso a los servicios y sistemas de información.

• Todos los funcionarios, contratista del fondo deben mantener controles de accesos eficientes, en particular con relación al uso de contraseñas, a la seguridad del equipo del usuario, al detener conservar escritorio y pantalla despejados para

reducir el riesgo de acceso no autorizado o daño de reportes, medios y servicios de procesamiento de Información.

• El proceso Gestión de TIC´S debe asegurar el bloqueo al acceso de páginas de contenido para adultos, redes sociales, hacking, descargas (FTP), mensajería instantánea y cualquier página que represente riesgo potencial para la Entidad mediante el uso de servidor proxy, firewall o el software que mejor se ajuste a la necesidad. Excepciones de acceso, serán aprobados por el jefe inmediato, según la necesidad del cargo y verificación previa de que las paginas solicitadas no contengan código malicioso con el visto bueno del oficial de seguridad de la información.

• El acceso a los sistemas operativos de la entidad deben estar protegidos por registros de inicio seguro, contemplando las siguientes condiciones no mostrar información del sistema, hasta que el proceso de inicio se haya completado, no suministrar mensajes de ayuda, durante el proceso de autenticación, validar los datos de acceso, una vez que se han diligenciado todos los datos de entrada, limitar el número de intentos fallidos de conexión auditando los intentos no exitosos, no mostrar las contraseñas digitadas, No transmitir la contraseña en texto claro.

• El uso de programas utilitarios debe ser limitado y minuciosamente controlado por el oficial de seguridad de la información con el objeto de garantizar la instalación de software no autorizado y cambios de configuración del sistema.

ARTÍCULO DECIMO SEPTIMO: POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

El FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA implementara y velara por la efectividad de los mecanismos de seguridad tanto físicos como de control de acceso, que permitan asegurar el perímetro de las instalaciones, a la vez que controlen las amenazas físicas tanto internas como externas y las condiciones de medio ambiente que se puedan presentar en las oficinas de la entidad.

A continuación se establecen las medidas de la política de Seguridad Física y del Entorno del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA:

- Garantizar la protección del perímetro de seguridad de las instalaciones físicas.

- Controlar el acceso a áreas restringidas tales como infraestructura de soporte de los sistemas de información**.**

- Todos los funcionarios , contratista y visitantes o terceras personas, que ingresen a las instalaciones del Fondo de Pasivo Social deberán poseer una identificación a la vista que claramente los identifique como tal.

ARTÍCULO DECIMO OCTAVO POLÍTICA DE GESTIÓN DE ACTIVOS

Los procesos de la entidad con el acompañamiento y asesora del Gestión TIC´S, deben, establecer la forma de identificación, uso, administración y responsabilidad frente a los activos de Información, con el fin de cumplir con los siguientes objetivos:

- Garantizar que los activos de información reciban un apropiado nivel de protección.

- Clasificar la información para señalar su criticidad, sensibilidad y reserva de la misma.

- Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

A continuación se establecen las medidas de la política de gestión de activos del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA:

- Identificar los activos de información de acuerdo a su tipo, su criticidad, sensibilidad y reserva de la misma, lo cual lo deben ser documentado y mantenido actualizados a la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información los responsables, los propietarios de la información o conocedor de los mismos dentro de la entidad centralizado por el proceso de gestión de TIC´S.

- El dueño o propietario de los activos de información, será el responsable de definir la categoría en la que cada activo de información se encuentra, así como determinar si es necesario un proceso de reclasificación y los controles requeridos para su protección.

- El uso de los activos de información pertenecientes al FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA es de responsabilidad del propietario asignado; es su deber proteger y mantener la confidencialidad, integridad y disponibilidad de los activos de información.

- Establecer los criterios y niveles de calificación de la información, para definir las medidas de protección adecuadas de los activos. Estos criterios se determinan de acuerdo con la confidencialidad, declarados en la ley 1712 del 2014 y la ley 1581 de 2012:

INFORMACION PÚBLICA RESERVADA: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley.

Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.

INFORMACION PUBCLCA CLASIFICADA: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley.

Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma.

Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.

INFORMACION PÚBLICA: Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.

Es aquella que puede ser accedida por cualquier persona, incluso por personas o entidades externas a la organización, con o sin vínculos laborales, comerciales, legales, entre otros.

NO CLASIFICADA: Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información.

DATO PÚBLICO: "Calificado como tal en la ley. Dato que no es semiprivado, privado o sensible (Ej. Datos relativos al estado civil de las personas, su profesión u oficio, su calidad de comerciante o servidor público y aquellos que pueden obtenerse sin reserva alguna)."

DATO SEMIPRIVADO: Dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento interesa al titular y a cierto sector o grupo de personas o a la sociedad en general (Ej. Datos financieros y crediticios, dirección, teléfono, correo electrónico).

DATO PRIVADO: Dato que solo es relevante para su titular (Ej. Fotografías, videos, datos relacionados con su estilo de vida.)

DATO SENSIBLE: Categoría especial de datos personales. Se consideran datos sensibles aquellos datos referidos a ideología, creencias, religión, afiliación sindical, salud, origen racial o vida sexual de las personas.

Su criticidad De acuerdo a las siguientes categorías:
Confidencialidad: Donde su valoración es alta si es información reservada, media en caso de que sea clasificada y baja si es pública.

Integridad: Donde su valoración será alta en caso de que sea información sea crítica o no crítica.

Disponibilidad: donde la valoración es alta, media o baja de acuerdo a su criticidad.

• Cada activo de información serán etiquetados de acuerdo con el esquema de clasificación aprobado por la entidad y teniendo en cuenta la tablas de retención documental establecidas en cada proceso.

• Definir un procedimiento para el etiquetado y manejo de la información de con el esquema de clasificación y teniendo en cuenta la tablas de retención documental establecidas en cada proceso el cual debe ser aprobado por la entidad.

ARTÍCULO DECIMO NOVENO: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

El proceso Gestión TIC´S y los responsables del tema de Seguridad de la información deben contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos frente a fallas, ataques o desastres**.**

A continuación se establecen las medidas de la política de seguridad de la información en la continuidad de las tecnologías de la información del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA:

• Seguir con la estrategia de recuperación establecida en el plan de contingencia de las tecnologías de la información y las comunicaciones (TIC), para asegurar la restauración de los procesos críticos del negocio, ante el evento de una contingencia.

• Contar con instalaciones alternas y con capacidad de recuperación, que permitan mantener la continuidad del negocio aún en caso de desastre en las instalaciones de los lugares de operación.

• Incluir los controles establecidos en cada una del proceso que se clasificaron críticos, para que no se vea disminuido los aspectos de seguridad en caso de desastre.

ARTÍCULO VIGÉSIMO POLÍTICA DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

El FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA proporcionará los mecanismos necesarios para garantizar la protección de la información y recursos de la plataforma tecnológica en donde almacena, procesa su información y la de sus afiliados, adoptando los controles que sean necesarios para evitar la modificación, daño o divulgación ocasionada por el contagio de software malicioso.

A continuación se establecen las medidas de la política de protección frente a software malicioso del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA:

- El proceso Gestión TIC´S debe proveer herramientas tales como software antivirus, antimalware, antispam, antispyware y demás (con las respectivas licencias de uso requeridas), que permitan reducir el riesgo de contagio de software malicioso y que a su vez respalden la seguridad de la información que se encuentra administrada y almacenada en la plataforma de la entidad.

- El proceso Gestión TIC´S, a través de su equipo de trabajo, debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de protección de software malicioso.

- Los usuarios deben asegurarse que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras.

- Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar al proceso Gestión TIC´S para que se tomen las medidas correspondientes.

ARTÍCULO VIGÉSIMO PRIMERO POLÍTICA DE COPIAS DE RESPALDO DE LA INFORMACIÓN

FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA garantizará la realización de copias de seguridad donde se respalde y almacene la información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades, adicionalmente, el proceso Gestión TIC´S, velara porque los medios magnéticos donde se almacene la información crítica, se encuentren en una ubicación distinta a las instalaciones donde se encuentra dispuesta, ubicación que debe contar con los controles de seguridad física y ambiental adecuados.

A continuación se establecen las medidas de la política copias de respaldo de la información del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA:

- El proceso Gestión TIC´S, a través de su equipo de trabajo debe generar y adoptar los procedimientos para el almacenamiento, generación, restauración y tratamiento de las copias de seguridad y respaldo de la información, buscando garantizar su integridad y disponibilidad.

- Es responsabilidad de los usuarios de la plataforma tecnológica de la entidad, el identificar la información considerada como crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

ARTÍCULO VIGÉSIMO SEGUNDO POLÍTICA DE GESTIÓN DE VULNERABILIDADES

El FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA a través del proceso Gestión TIC´S revisará de forma periódica la aparición de vulnerabilidades técnicas sobre los recursos de la entidad por medio de la realización periódica de pruebas de vulnerabilidades.
A continuación se establecen las medidas de la política de gestión de vulnerabilidades del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA:

- El proceso Gestión TIC´S debe revisar de forma periódica la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la respectiva plataforma así como de los administradores de los sistemas de información con el fin de prevenir la exposición al riesgo de estos.

• El proceso Gestión TIC´S a través de su equipo de trabajo debe generar y ejecutar o monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica de la entidad.

ARTÍCULO VIGÉSIMO TERCERO POLÍTICA PARA EL TRATAMIENTO DE DATOS PERSONALES

En cumplimiento de la de Ley 1581 de 2012y su decreto reglamentario, por la cual se dictan disposiciones para la protección de datos personales, el FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA, como custodio, responsable y/o encargado del tratamiento de datos personales, garantizara la protección de los datos personales de sus afiliados, proveedores y/o terceros recibida a través de los diferentes canales de recolección de información y hará uso de los mismos únicamente para las finalidades para las que se encuentra facultado, especialmente las señaladas a continuación:

• Reconocer las prestaciones económicas y ordenar el respectivo pago.

• Para el reporte de estadísticas que alimentan el sistemas de salud a los entes rectores y de control como Ministerio de Salud y Protección Social, Supersalud - Superintendencia Nacional de Salud, Secretarias de Salud.

• Para los fines administrativos propios de la entidad.

• Para la administración y prestación de los servicios de salud a los obligado a prestar.

• Caracterizar ciudadanos y grupos de interés y adelantar estrategias de mejoramiento en la prestación del servicio.

• Dar tratamiento y respuesta a las peticiones, quejas, reclamos, denuncias, sugerencias y/o felicitaciones presentados a la entidad.

• Alimentar el Sistema de Información y Gestión de Empleo Público –SIGEP.

- Asuntos jurisdiccionales.

Deberes del responsable del tratamiento Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

- Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

- Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular.

- Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.

- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.

- Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.

- Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.

- Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley.

- Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.

- Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley;

- Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos.

- Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.

- Informar a solicitud del Titular sobre el uso dado a sus datos.

- Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

- Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

A continuación se establecen las medidas de la política de protección de datos personales del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA:

- El fondo realiza el tratamiento de Datos Personales en ejercicio propio de sus funciones legales y para el efecto no requiere la autorización previa, expresa e informada del Titular. Sin embargo, cuando no corresponda a sus funciones deberá obtener la autorización por medio de un documento físico, electrónico, mensaje de datos, Internet, sitio web, o también de manera verbal o telefónica o en cualquier otro formato y mantendrá las pruebas de ésta para su posterior consulta.
- Los Datos Personales que hayan sido sometidos a Tratamiento deberán ser exacto, completo, veraz, actualizado, comprobable y comprensible.

- El fondo conservará la información bajo estas características siempre y cuando el titular informe oportunamente sus novedades y serán tratados por aquellos Funcionarios del Fondo que cuenten con el autorización para ello, o quienes dentro de sus funciones tengan a cargo la realización de tales actividades o por los Encargados.

- Los datos personales sometidos a Tratamiento se les deben proveer las medidas humanas y técnicas para su protección garantizando su seguridad de que no puedan ser divulgados, modificados accedidos sin previa autoriza dación, eliminados o se entrega terceros sin autorización del titular.

- En caso de delegar a un tercero para el tratamiento de datos personales, la entidad exigirá a este la correcta implementación de lineamientos y procedimientos necesarios para salvaguardar la integridad y protección de los datos personales y garantizar que la información que le suministre sea veraz, completa, exacta, actualizada, comprobable y comprensible. Adicionalmente le comunicará de manera oportuna todas las novedades a que haya lugar para que la información siempre se mantenga actualizada.

- El fondo registra las bases de datos en el Registro Nacional de Base de Datos RNBD – en cumplimiento a los establecido en la ley 1581 de 2012.

- El Titular de los datos personales puede ejercer, principalmente, sus derechos mediante la presentación de consultas y reclamos ante la SIC, en su sede cuyo domicilio es la carrera 13 No. 18 – 24 en el proceso de Atención al Ciudadano y por el correo electrónico quejasyreclamos@fps.gov.co.

- El incumplimiento de la política de tratamiento de datos personales acarreara sanciones contempladas en el código único disciplinario y normas relacionadas.

- El fondo implementara procedimiento para garantizar el cumplimiento de la Política de tratamiento de datos personales.

-

CAPITULO IV REVISION, INCUMPLIMIENTO Y VIGENCIA

ARTÍCULO VIGECIMO CUARTO REVISIÓN Y MEDICIÓN

La Política General de Seguridad y Privacidad de la Información será revisada o evaluada su cumplimiento semestralmente o cuando requiera modificaciones con el objeto de mantenerla actualizada Este proceso será liderado por gestión TIC´S, y revisado por la oficina de planeación y sistemas y aprobado por el comité de desarrollo administrativo, considerando los siguientes aspectos:

- Condiciones contractuales, reguladora y legales.

- Cambios en ámbito organizacional o técnico.

- Disponibilidad de recursos.

- Retroalimentación de las parte 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.

ARTÍCULO VIGECIMO QUINTO INCUMPLIMIENTO

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

ARTÍCULO VIGECIMO SEXTO VIGENCIAS

La presente resolución rige a partir de la fecha de su expedición.

COMUNICASE Y CUMPLASE:
JAIME LUIS LACOUTURE PEÑALOZA
Director General

ANEXO C. Guía metodológica de análisis de riesgos de seguridad y privacidad de la información FPS

GUÍA METODOLÓGICA DE ANÁLISIS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Fecha de Vigencia: DD / MM / AA

CONTROL DE DOCUMENTOS			
Elaborado por: Roselys Silva Cuadrado	**Cargo:** Profesional	**Fecha:** **Agosto/31/2016**	**Firma:**
Revisado Técnicamente en OPS:	**Cargo:**	**Fecha:**	**Firma:**
Aprobado Mediante **Acta No :** **Acto Administrativo:** **Fecha:**			

CONTROL DE CAMBIOS:			
Versión	**Fecha y acto administrativo de aprobación**	**Cambio**	**Nombre del solicitante**
1.0			Mauricio Villaneda Jiménez

1. OBJETIVO

Definir la metodológica de análisis de riesgo de seguridad y privacidad de la información contemplando: identificación de activos de información, amenazas, vulnerabilidades, riesgos y controles, los niveles aceptables y tratamiento de riesgo en el Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia , teniendo en cuenta los lineamientos descritos en la Norma Técnica Colombiana NTC ISO 31000.

2. ALCANCE

La Guía Metodológica de Análisis de Riesgos de Seguridad y privacidad de la Información provee los mecanismos necesarios para identificar, analizar, evaluar y tratar de manera adecuada los riesgos asociados a los activos de información del Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia.

3. BASES LEGALES

Circular Externa 042 de 2012.

Lineamientos establecidos en la Norma ISO/IEC 27001.

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).

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).

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).

Vulnerabilidad

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

5. METODOLOGIA DE GESTIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la metodología de evaluación y tratamiento de riesgo es importante realizar un análisis inicial relacionado con el estado actual de la estructura de riesgo y la gestión en la entidad, desde el punto de vista estratégico; para ello se estructura la siguiente metodología en el cuadro 8:

Cuadro 8. Etapas de la gestión del riesgo a lo largo del MSPI

Etapas del modelo de seguridad y privacidad de la información	**Proceso de gestión en la seguridad de la información**
Planear	Establecer contexto Planificación del tratamiento del riesgo Aceptación del riesgo
Implementar	Implementación del plan de tratamiento de riesgo
Gestionar	Monitoreo y revisión continuo de los riesgos
Mejora continua	Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información
Fuente: Guía de gestión de riesgos del Ministerio de Tecnologías de la Información y las Comunicaciones	

5.1 ESTABLECIMIENTO DE CONTEXTO

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 y privacidad de la información,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.

Criterios de Evaluación del Riesgo

- El valor estratégico del proceso de información del negocio.

- Criticidad de los activos involucrados.

- Requisitos legales y reglamentarios, así como las obligaciones contractuales.

- La importación de la disponibilidad confidencialidad e integridad para las operaciones y el negocio.

- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación.

Criterios de Impacto

- Nivel de clasificación de los activos de información impactados.

- Brechas en la seguridad de la información (por ejemplo, pérdida de confidencialidad, integridad y disponibilidad).

- Operaciones deterioradas (partes internas o terceras partes).

- Perdida del negocio y valor financiero.
- Alteración de planes y fechas límites.
- Daños para la reputación.
- Incumplimiento de los requisitos legales, reglamentarios o contractuales.

Criterios de Consecuencias

- Incumplimiento de la legislación y/o reglamentación.
- Perdida del buen nombre/efecto negativo en la reputación.
- Efectos adversos en el cumplimiento de la ley.
- Alteración de las actividades de la entidad.
- Interrupción de servicios.
- Incapacidad para prestar servicio.
- Alteración de la operación interna.
- Costo interno adicional.
- Alteración en la operación de una tercera parte.
- Incapacidad para cumplir las obligaciones contractuales.

- Incumplimiento a contrato.

- Peligro para el personal/seguridad del usuario.

- Procesos judiciales y castigo.

Evaluación del Impacto

- El valor financiero del reemplazo del activo perdido (o parte de este activo).

- El costo de adquisición, configuración e instalación del activo nuevo o de su copia de soporte.

- El costo de las operaciones suspendidas debido al incidente hasta que se restaure el servicio prestado por el (los) activos(s).

- El impacto tiene como resultado una brecha de seguridad en la información.

- Costo de la oportunidad (nuevos recursos financieros necesarios para reemplazar o reparar un activo se podrían haber utilizado en otra parte).

- El costo de las operaciones interrumpidas.

- El potencial de la mala utilización de la información obtenida a través de una brecha de seguridad.

- Incumplimiento de las obligaciones estatutarias o reglamentarias.

- Incumplimiento del código de ético de conducta.

Criterio de Aceptación del Riesgo

Durante la etapa de evaluación de riesgos se aceptan aquellos riesgos de zona de riesgo “baja” y “moderada”, y no se aceptan los riesgos de zona “Alto” y “externa” los cuales deben ser tratados o transferirlos y se aceptará el riesgo siempre y cuando el costo beneficio sea negativo y no afecte la política de seguridad.

Así, se puede seguir definiendo otros criterios de aceptación de riesgos los cuales se emplearán durante el tratamiento.

Por ello la entidad teniendo en cuenta los criterios anteriormente mencionados se establece en los cuadros 9 y 10, de manera cuantitativa y cualitativa los criterios de evaluación del riesgo, criterios de impacto, de probabilidad.

Cuadro 9. Establecimiento de criterios

Nivel	Niveles para calificar el Impacto	Impacto (consecuencias) Cuantitativo	Impacto (consecuencias) Cualitativo
5	Catastrófico	Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor mayor o igual al 50% del Presupuesto general de la entidad. Pago de reconocimientos de prestaciones económicas a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor mayor o igual al 50%.	Interrupción de las operaciones de la Entidad mayor a un mes. Intervención por parte de un ente de control u otro ente regulador. Pérdida de Información crítica para la entidad que no se puede recuperar. Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. Imagen institucional afectada en el orden nacional por actos o hechos de corrupción comprobados. Daño reputacional desastroso con los ciudadanos o con otras entidades.
4	Mayor	Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor mayor o igual al 20% del presupuesto general de la entidad. Pago de reconocimientos de prestaciones económicas a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor mayor o igual al 20%	Interrupción de las operaciones de la Entidad por una semana a un mes Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. Sanción por parte del ente de control u otro ente regulador. Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. Imagen institucional afectada en el orden nacional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos. Daño reputacional grave con los ciudadanos o con otras entidades.

Cuadro 9. (Continuación)

Nivel	Niveles para calificar el Impacto	Impacto (consecuencias) Cuantitativo	Impacto (consecuencias) Cualitativo
3	Moderado	Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor mayor o igual al 5% del presupuesto general de la entidad. Pago de reconocimientos de prestaciones económicas a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor mayor o igual al 5%.	Interrupción de las operaciones de la Entidad de un día a una semana Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. Reproceso de actividades y aumento de carga operativa. Imagen institucional afectada en el orden nacional por retrasos en la prestación del servicio a los usuarios o ciudadanos. Investigaciones penales, fiscales o disciplinarias. Daño reputacional importante con los ciudadanos o con otras Entidades.
2	Menor	Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor menor al 5% del presupuesto general de la entidad. Pago de reconocimientos de prestaciones económicas a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor menor al 5%.	- Interrupción de las operaciones de la Entidad por medio día o un día - Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos. Daño reputacional apreciable con los ciudadanos o con otras Entidades.
1	Insignificante	Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor menor o igual al 1% Pago de reconocimientos de prestaciones económicas a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor menor o igual al 1%.	Interrupción de las operaciones de la entidad menos de medio día. No se generan sanciones económicas o administrativas. No se afecta la imagen institucional de forma significativa. No habría Daño reputacional con los ciudadanos o con otras Entidades.
Fuente: Autores			

Cuadro 10. Criterio de probabilidad

Nivel	Descriptor	Descripción	Frecuencia
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de una vez al año.
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de una vez en el último año.
3	Posible	El evento podría ocurrir en algún momento.	Al menos de una vez en los últimos 2 años.
2	Improbable	El evento puede ocurrir en algún momento	Al menos de una vez en los últimos 5 años.
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años
Fuente: Guía de riesgo del Departamento Administrativo de la Función Pública			

5.2. VALORACIÓN DEL RIESGO

5.2.1 Identificación de riesgos Esta actividad se realiza con base a las causas internas o externas identificadas por los procesos a través del contexto estratégico, describiendo cuales son los activos críticos asociados a los procesos y cuales contienen información sensible, para ello es necesario definir los siguientes términos que permite la establecimiento de esta actividad, y se listaran a continuación:

- Proceso
- Objetivo del proceso
- Identificación de activos críticos
- Riesgo
- Causas (amenazas y vulnerabilidades)
- Descripción del riesgo

- Efectos de la materialización del Riesgo

5.2.2 Identificación y clasificación de los activos La identificación del activo y de sus componentes es el primer paso para el desarrollo de un análisis de riesgos. Se Identifican únicamente los activos críticos; para la clasificación de los activos de información se debe considerar la importancia de la información que es almacenada, procesada o transmitida por dicho activo; por ejemplo, si un servidor procesa información clasificada como crítica, entonces el servidor será considerado como crítico.

Los activos serán clasificados de acuerdo a la política de gestión de activos y al procedimiento respectivo: APGTSOPSPTXX INVENTARIO, CLASIFICACIÓN Y ETIQUETADO DE ACTIVOS DE INFORMACIÓN.

5.2.3 Identificación y clasificación de las amenazas Las amenazas son las situaciones o eventos de las cuales debe proteger a los activos de información de la entidad. Las amenazas se identifican y se clasifican en las siguientes clases:

De origen natural: Inundaciones, terremotos, incendios, rayos.

Fallos de la infraestructura auxiliar: Fallos de suministro eléctrico, refrigeración, contaminación.

Fallos de los sistemas informáticos y de comunicaciones: Fallos en las aplicaciones, hardware o equipos de transmisiones.

Error humano: errores accidentales o deliberados de las personas que interactúan con la información, por ejemplo: acciones no autorizadas como uso de software o hardware no autorizados o funcionamiento incorrecto por abuso o robo de derechos de acceso o errores en el uso, falta de disponibilidad, o información comprometida por robo de equipos, desvelado de secretos, espionaje.

Cada propietario de la información identificara y clasificara las amenazas a la que eta sujeta el activo de acuerdo a las clases anteriormente mencionadas y darle su impacto ayudándose con las siguientes preguntas:

- ¿Qué valor tiene este activo para la empresa?

- ¿Cuánto cuesta su mantenimiento?

- ¿Cómo repercute en los beneficios de la empresa?

- ¿Cuánto valdría para la competencia?

- ¿Cuánto costaría recuperarlo o volverlo a generar?

- ¿Cuánto costó adquirirlo o su desarrollo?

- ¿A qué responsabilidades legales o contractuales nos enfrentamos si se ve comprometido?

5.2.4 Identificación de las vulnerabilidades Para realizar esta instancia se tienen en cuenta las listas de amenazas, de activos de información y controles existentes en las etapas anteriormente mencionadas.

Las vulnerabilidades serán identificadas de acuerdo a los factores intrínsecos a los activos, es decir la naturaleza de los mismos por ejemplo: localizaciones que son más propensas a desastres naturales como por ejemplo inundaciones o que están en lugares con variaciones de suministro eléctrico y de acuerdo a las siguientes áreas:

- Organización.

- Procesos y procedimientos.

- Rutinas de gestión.

- Personal

- Ambiente físico

- Configuración del sistema de información.

- Hardware, software y equipos de comunicaciones.

- Dependencia de partes externas

- Finalmente se tendrá un listado de las vulnerabilidades identificadas relacionadas con los activos, las amenazas y controles.

5.2.5 Identificación de controles existentes En esta instancia para la identificación de controles existentes se deben tener en cuenta las siguientes actividades:

- Revisar los documentos que contengan información sobre los controles.

- Verificación con las personas responsables de la seguridad de la información y los usuarios.

- Efectuar revisiones en sitio comparando los controles implementados contra la lista de controles que deberían estar.

- Cuáles están implementados correctamente y si son o no eficaces.

- Revisión de los resultados de las auditorías internas.

Lo anterior con el objeto de garantizar que los controles funcionen correctamente y reducen la probabilidad de ocurrencias de la amenaza y la facilidad de explotar la vulnerabilidad o el impacto del incidente.

5.2.6 Identificación de las consecuencias Es decir, cómo estas amenazas y vulnerabilidades afectan a la disponibilidad, integridad y confidencialidad de los activos de información teniendo en cuenta el impacto aspecto económico, organizacional, credibilidad o imagen, legal, operativo.

5.2.7 Análisis del riesgo La Guía para la Administración del Riesgo del DAFP7 instituye que en el análisis de riesgo busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto. Con el fin de estimar la zona de riesgo inicial, denominada como riesgo inherente. Para ello se mide las consecuencias o impactos de la pérdida de confidencialidad, integridad y disponibilidad teniendo en cuenta los criterios establecidos en el ítem de aceptación del riesgo, se estima la probabilidad entendida como la posibilidad de ocurrencia del riesgo o incidentes, con ello podemos estimar el nivel de riesgo inicial, cruzando los valores establecidos para la probabilidad y el impacto o consecuencias con el objeto de establecer la zona de riesgo en la cual se ubica el riesgo identificado. Esto se denomina riesgo inherente y se define como aquél al que se enfrenta una entidad en ausencia de acciones o controles por parte de la Dirección para modificar su probabilidad o impacto.

5.2.8 Evaluación de riesgo En esta fase busca confrontar los resultados del análisis de riesgo para determinar los riesgos aceptables, tolerables, moderados, importantes o inaceptables y fijar las prioridades de las acciones requeridas para su tratamiento. Se genera de una comparación en la cual se presenta el análisis de la probabilidad de ocurrencia del riesgo versus el impacto o consecuencias del mismo, se obtiene al final la matriz denominada “Matriz de Calificación, Evaluación y respuesta a los Riesgos” de esta forma se califica 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 el siguiente cuadro 11:

Cuadro 11. Matriz de Calificación, Evaluación y respuesta a los Riesgos

CASI SEGURO	***5***	**A**	**A**	**E**	**E**	**E**
PROBABLE	***4***	**M**	**A**	**A**	**E**	**E**
POSIBLE	***3***	**B**	**M**	**A**	**E**	**E**
IMPROBABLE	***2***	**B**	**B**	**M**	**A**	**E**
RARO	***1***	**B**	**B**	**M**	**A**	**A**
PROBABILIDAD		***1***	***2***	***3***	***4***	***5***
		INSIGNIFICANTE	***MENOR***	***MODERADO***	***MAYOR***	***CATASTROFICO***
		IMPACTO				
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 el Riesgo						
E: Zona de Riesgo Extrema: Reducir el Riesgo, Evitar, Compartir o Transferir el Riesgo						
Fuente: Guía de riesgo del Departamento Administrativo de la Función Pública						

Adicionalmente se valoriza el riesgo realizando un producto de confrontar los resultados de la evaluación del riesgo con los controles identificados y establecidos, esto se hace con el objetivo de establecer nuevos controles que permitan mitigar los riesgos, en la definición de éstos nuevos controles, se utiliza el cuadro 12 de "estructura de controles" que presenta la guía de controles del MSPI, para hacer un trabajo documentado y ordenado.

Cuadro 12. Estructura de controles

Política general			
Número	Nombre	Seleccionado / Excepción	Descripción / Justificación
	Nombre	Control	
Fuente: Guía – Controles del MSPI			

Por otro lado, hacer una clasificación y valoración de los controles, teniendo en cuenta la *determinación la naturaleza del control es decir tipo de Control Preventivo y Correctivo* definidos como se indica a continuación:

• Preventivos: aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización.

• Correctivos: aquellos que permiten el restablecimiento de la actividad, después de ser detectado un evento no deseable; también la modificación de las acciones que propiciaron su ocurrencia.

Establecer si los controles están 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.

Establecer si el control que se implementa es automático o manual.

Controles automáticos: Utilizan herramientas tecnológicas como sistemas de información o software que permiten incluir contraseñas de acceso, o con Controles de seguimiento a aprobaciones o ejecuciones que se realizan a través de éste, generación de reportes o indicadores, sistemas de seguridad con scanner, sistemas de grabación, entre otros. Este tipo de controles suelen ser más efectivos en algunos ámbitos, dados su complejidad.

Controles manuales: Políticas de operación aplicables, autorizaciones a través de firmas o confirmaciones vía correo electrónico, archivos físicos, consecutivos, listas de chequeo, controles de seguridad con personal especializado, entre otros.

Establecer si los controles se están aplicando en la actualidad y si han sido efectivos para minimizar el riesgo.

Una vez haya clasificado los controles y haya determinado si están documentados si el control que se implementa es automático o manual se están aplicando en la actualidad y si han sido efectivos para minimizar el riesgo se procede a realizar la valoración de la que se tuvo en cuenta la herramienta definida por el DAFP y que se ajustó a las necesidades y lineamientos que requiere el Fondo de la siguiente manera en los cuadro 13 y 14:

Cuadro 13. Valoración de controles

Parámetros	Criterios	Tipo de control		Puntajes
		Probabilidad	Impacto	
Herramientas para ejercer el control	Posee una herramienta para ejercer el control			15
	Existen manuales, instructivos o procedimiento para el manejo de la herramientas			15
	En el tiempo que lleva la herramienta ha demostrado ser efectiva			30
Seguimiento al control	Esta definidos los responsables de la ejecución del control y del seguimiento			15
	La frecuencia de la ejecución del control y seguimiento es adecuada			25
	Total			100
Fuente: Guía de Riesgos del DAFP				

Cuadro 14. Rangos de calificación de los controles

Rangos de calificación de los controles	Dependiendo si el control afecta probabilidad o impacto desplaza en la matriz de calificación, evaluación y respuesta a las riesgo	
	Cuadrantes a disminuir en la probabilidad	Cuadrantes a disminuir en el impacto
Entre 0 -50	0	0
Entre 51 – 75	1	1
Entre 76 - 100	2	2
Fuente: Guía de Riesgos del DAFP		

5.2.9 Tratamiento del riesgo En este paso se toman los resultados de la etapa anterior donde se ha establecido la zona de riesgo determinada por el desplazamiento dentro de la Matriz de Evaluación y Calificación y la nueva valoración de acuerdo a los controles identificados y esta manera se determinará finalmente la selección de las opciones de tratamiento del riesgo, así:

- Evitar el riesgo decidiendo no iniciar o continuar la actividad que lo originó.

- Tomar o incrementar el riesgo con el fin de perseguir una oportunidad.

- Retirar la fuente del riesgo.

- Cambiar la probabilidad.

- Cambiar las consecuencias.

- Compartir el riesgo con una o varias de las partes (incluyendo los contratos y la financiación del riesgo).

- Retener el riesgo a través de la decisión informada.

- Teniendo en cuenta equilibro del costo y el esfuerzos de la implementación frente a los beneficios derivados con respecto a los requisitos legales, reglamentarios y otros, como la responsabilidad social y la protección del medio ambiente.

6. PLAN DE IMPLEMENTACIÓN

En esta fase se debe seleccionar y justificar las acciones que implementara para cada riesgo identificado, los responsables de esta implementación. A este plan se añadirá una relación de riesgos residuales, es decir, aquellos que aún siguen existiendo a pesar de las medidas tomadas.

El plan de implementación y los riesgo residual deberá aprobados por los proceso antes de ser aceptado por alta dirección.

7. MONOTOREO Y REVISION

El monitoreo y revisión es un fase que permite asegurar que las acciones y controles que han implementado son eficientes y para evidenciar todas aquellas situaciones que puede interviniendo en la aplicaciones de acciones preventivas.

Por ello periódicamente se revisará:

- Nuevos activos o modificaciones en el valor de los activos.

- Nuevas amenazas.

- Cambios o aparición de nuevas vulnerabilidades.

- Aumento de las consecuencias o impactos.

- Incidentes de seguridad de la información.

- Probabilidades en busca de posibles cambios.

- De forma paralela se revisará el propio proceso de gestión de riesgos para adecuarlo al contexto. Esta revisión afecta entre otros a:

- Las categorías de activos.

- Los criterios de evaluación de riesgos.

- Los niveles de clasificación de los impactos.

- Las escalas de aceptación de riesgos.

- Los recursos necesarios.

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.

8. POLÍTICAS DE ADMINISTRACIÓN DEL RIESGO

Se tendrán en cuenta las establecidas por el Fondo para gestión del riesgo del sistema de gestión de MECI y Calidad, complementa de la definición de la declaración de aplicabilidad (SOA), el cual es el documento con las justificaciones de la aplicación o elección de los controles, de por qué no se eligieron los controles que hayan quedado por fuera, después del plan de tratamiento de riesgos.

9. ANEXOS

Cuadro 15. Listado de Amenazas

A	Accidental
D	Deliberada
E	Ambiental

TIPO	AMENAZA	ORIGEN
Daño físico	Fuego	A, D, E
	Daño por Agua	A,D, E
	Polvo, Corrosión, Congelamiento	A, D, E
	Destrucción de Equipos o Medios	A,D, E
Eventos Naturales	Fenómenos Climáticos	E
	Fenómenos Sísmicos	E
	inundación	E
Perdida de los Servicios esenciales	Falla en el suministro de Agua o de aire acondicionado	A,D
	Perdida de Suministro de Energía	A,D, E
	Falla en equipo de telecomunicaciones	A,D
Perturbación debida a la radiación	Perturbación debida a la radiación electromagnética	A, D, E
Compromiso de la Información	Espionaje remoto	D
	Piratería	D
	Ingeniería social	D
	Accesos no autorizados a los sistemas	D
	Escucha Subrepticia	D
	Suplantación de Identidad	D
	Hurto de medios o documentos	D
	Hurto de Equipo	D
	Recuperación de Medios reciclados o Desechados	D
	Divulgación	A,D
	Datos provenientes de fuentes no confiables	A, D
	Manipulación con Hardware	D
	Manipulación con software	A,D
	Software Malicioso	D

Cuadro 15. (Continuación)

Fallas Técnicas	Falla del equipo	A
	Mal funcionamiento de equipo	A
	Saturación del sistema de información	A, D
	Mal funcionamiento del software	A
	Incumplimiento en el mantenimiento del sistema de información A	D
	Incumplimiento en el mantenimiento de equipo	A, D
Acciones no autorizadas	Uso no autorizado de Equipos	A, D
	Copia fraudulenta de software	D
	Uso de Software falso o copiado	A,D
	Corrupción de los datos	D
	Procesamiento ilegal de los datos	D
	Allanamiento Ilegal	A,D

Cuadro 16. Listado de vulnerabilidades

Mantenimiento insuficiente/instalación fallida de los medio de almacenamiento
Falta de esquemas de reemplazo periódico. Susceptibilidad a la humedad, el polvo y la suciedad.
Falta de control de cambio con configuración eficiente
Susceptibilidad a las variaciones de tensión
Almacenamiento sin protección
Falta de cuidado en la disposición final
Copia no controlada
Falta de "terminación de la sesión" cuando se abandona la estación de trabajo
Disposición o reutilización de los medios de almacenamiento sin borrado adecuado
Falta de mecanismos de identificación y autentificación , como la autentificación de usuario
Gestión deficiente de las contraseñas
Software nuevo o inmaduro
Descarga y uso no contralados de software
Falta de copias de respaldo
Falta de protección física de las puertas y ventanas de la edificación
Conexión deficiente de los cables

Cuadro 16.(Continuación)
Punto único de falla
Arquitectura e infraestructura insegura de la red
Transferencias de contraseña autorizada
Falta de conciencia acerca de la seguridad
Falta de mecanismos de monitoreo
Trabajo no supervisado del personal externo o de la limpieza
Falta de políticas para el uso correcto de los medio de telecomunicaciones y mensajería
Uso inadecuado o descuido del control físico de acceso físico a las edificaciones y los recintos
Red energética inestable
Falta de procedimiento formal para la autorización de la información disponible al publico
Falta de planes de continuidad
Falta de políticas sobre el uso del correo electrónico
Falta de procedimiento para el manejo de información clasificada
Falta de procesos disciplinarios definidos en la caso de incidentes de seguridad en la información
Falta de políticas formal sobre utilización de computadores portátiles
Falta de control de los activos que se encuentran fuera de las instalaciones
Falta o insuficiencia de política sobre limpieza de escritorio y de pantalla
Falta de mecanismos de monitoreo establecidos para las brechas en la seguridad
Falta de procedimientos para la presentación de informes sobre las debilidades en la seguridad
Falta de procedimiento del cumplimiento de las disposiciones con los derechos intelectuales.

10. BIBLIOGRAFÍA

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA, Guía para la Administración del Riesgo del Departamento Administrativo de la Función Pública (DAFP). Disponible en web www.dafp.gov.co.

ICONTEC, NTC-ISO 27001:2013 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

Anexo D. Inventario Activos Datos- Información FPS

Cuadro 17. Activos de información identificados

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
SERVICIOS	Módulo de Peticiones, Quejas y Reclamos	El detalle de la información referente al activo es la siguiente: Peticiones, Quejas , Reclamos, Sugerencias y Denuncias a nivel nacional Recepcionadas por los diferentes canales - Bases de datos del programa de correspondencia	Ciudadanos	Si	Español	Electrónico	Se encuentra en BD	Disponible	Publicada	Gestión Tic´s	Atención al Ciudadano	PÚBLICA	DATO PÚBLICO	Bajo	Medio	Alto
ACTIVO DE INFORMACION	Peticiones, Quejas , Reclamos, Sugerencias y Denuncias-PQRSD	El detalle de la información referente al activo es la siguiente: Peticiones, Quejas , Reclamos, Sugerencias y Denuncias a nivel nacional Recepcionadas por los diferentes canales - Serie documental, la cual puede tener la siguiente información: PQRSD Recepcionadas por aplicativo supersalud, línea telefónica, vía correo electrónico, presencial y/o página web 220 79 .04 PETICIONES,QUEJAS,RECLAMOS,SUGERENCIAS Y DENUNCIAS	IPS prestadoras de servicios de salud, Ministerio de Salud y la Protección Social, Superintendencia nacional de salud y ciudadanos	Si	Español	Análogo o digital	Se encuentra en BD	Disponible	No Publicada	Atención al Ciudadano	Atención al Ciudadano	PÚBLICA CLASIFICADA o USO INTERNO	DATO SENSIBLE	Alto	Medio	Bajo
ACTIVO DE INFORMACION	Informes de Gestión	El detalle de la información referente al activo es la siguiente: Informes que evidencian las gestión del proceso	IPS prestadoras de servicios de salud, Ministerio de Salud y la Protección Social y ciudadanos	No	Español	Físico - papel	Papel	Disponible	Publicada	Atención al Ciudadano	Atención al Ciudadano	PÚBLICA	DATO PÚBLICO	Bajo	Medio	Alto

Cuadro 17. (Continuación)

ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	
VERSIÓN: 1.0	CÓDIGO:	FECHA ACTUALIZACIÓN:

PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	Informe de medición de la satisfacción al ciudadano	El detalle de la información referente al activo es la siguiente: Encuesta Percepción de la satisfacción al ciudadano, Encuesta de satisfacción pos trámite, Estadística de Terminales de Calificación - Serie documental, la cual puede tener la siguiente información: - Informe de medición de la satisfacción al ciudadano - 220 36 .01	Ciudadanos	No	Español	Físico - papel	Papel	Disponible	Publicada	Atención al Ciudadano	Atención al Ciudadano	PÚBLICA	DATO PÚBLICO	Bajo	Medio	Medio
ACTIVOS DE SOFTWARE	Quick Time	El detalle de la información referente al activo es la siguiente: Estadística de Terminales de Calificación - Bases de datos	Ciudadanos	No	Español	Electrónico	Se encuentra en BD	Disponible	No Publicada	Gestión Tic´s	Atención al Ciudadano	PÚBLICA	DATO PÚBLICO	Bajo	Medio	Alto
ACTIVO DE INFORMACION	Actas de comité de archivos	El detalle de la información referente al activo es la siguiente: Actas de realizadas por comité de archivo -Serie documental, la cual puede tener la siguiente información: Comité de Archivo - 220 08 .02	Todos los procesos	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión Documental	Gestión Documental	PÚBLICA	DATO PÚBLICO	Bajo	Medio	Medio
ACTIVO DE INFORMACION	Tabla de retención documental	El detalle de la información referente al activo es la siguiente: Actualización de las tablas de retención documental -Serie documental, la cual puede tener la siguiente información: Actualización de las tablas de retención documental - Soportes Gestión Documenta 220 52 .02	Todos los procesos	No	Español	Electrónico	Se encuentra en BD	Disponible	No Publicada	Gestión Documental	Gestión Documental	PÚBLICA	DATO PÚBLICO	Bajo	Medio	Medio

Cuadro 17. (Continuación)

ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	
VERSIÓN: 1.0	CÓDIGO:	FECHA ACTUALIZACIÓN:

PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACIO N	Transferencias documentales	El detalle de la información referente al activo es la siguiente: Transferencia de archivo de gestión - Serie documental, la cual puede tener la siguiente información: Actualización de las tablas de retención documental - Soportes Gestión Documental 220 52 .02	Todos los procesos	No	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión Documental	Gestión Documental	PÚBLICA	DATO PÚBLICO	Bajo	Medio	Medio
ACTIVOS DE SOFTWARE	DOCPLUS	El detalle de la información referente al activo es la siguiente: Transferencia documentales de los archivo de gestión por año - Bases de datos de transferencia documental	Todos los procesos	No	Español	Electrónico	Se encuentr a en BD	Disponible	No Publicada	Gestión Documental	Gestión Documental	PÚBLICA CLASIFICAD A o USO INTERNO	DATO SEMIPRIVA DO	Alto	Medio	Medio
ACTIVOS DE SOFTWARE	ORFEO	El detalle de la información referente al activo es la siguiente: Programa de gestión documental -Servidor que contiene la radicación y a vitalización de documentos y un servidor del módulo de PQRDS	Todos los procesos	Si	Español	Electrónic o	Se encuen tra en BD	Disponible	No Publicada	Gestión Tic´s	Gestión Document al	PÚBLICA RESERVA DA	DATO SEMIPRIV ADO	Alto	Alto	Alto
ACTIVO DE INFORMACI ON	Inventario documental	El detalle de la información referente al activo es la siguiente: conjunto de documentos que conforman el archivo central de la entidad	Todos los procesos	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión Documental	Gestión Document al	PÚBLICA CLASIFIC ADA o USO INTERNO	DATO SEMIPRIV ADO	Alto	Alto	Medio
ACTIVOS DE SOFTWARE	Prestamos Documentales	El detalle de la información referente al activo es la siguiente: Control de préstamos de unidades documentales del archivo de Central - Serie documental, la cual puede tener la siguiente información: Formato préstamo documentos archivo gestión - 220 52 .02 SOPORTES GESTION DOCUMENTAL	Todos los procesos	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión Documental	Gestión Document al	PÚBLICA	DATO PÚBLICO	Bajo	Medio	Alto

Cuadro 17. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	Informes de Gestión	El detalle de la información referente al activo es la siguiente: Informes que evidencian las gestión del proceso - Serie documental, la cual puede tener la siguiente información: - Informe de desempeño - Informe de gestión - 220 53 .09	Todos los procesos	No	Español	Físico - papel	Papel	Disponible	Publicada	Gestión Documental	Gestión Documental	PÚBLICA	DATO PÚBLICO	Bajo	Medio	Medio
ACTIVOS DE SOFTWARE	Aplicativo SAFIX	El detalle de la información referente al activo es la siguiente: Sistema de información que manera la novedades, nominas Generador de reportes de los pensionados (ferrocarriles nacionales, Prosocial, fundación san Juan de dios y materno infantil)	Gestión de tics, Tesorería, Contabilidad	Si	Español	Electrónico	Se encuentra en BD	Disponible	No Publicada	Gestión Tic´s	Gestión de Prestaciones Económicas	PÚBLICA RESERVADA	DATO SEMIPRIVADO	Alto	Alto	Alto
ACTIVO DE INFORMACION	ACCION DE TUTELA	El detalle de la información referente al activo es la siguiente: Documentación sobre conculcación de acción, contestación, fallos, incidente de desacato - subserie documental que contiene la siguiente documentación: Oficio de respuesta tutela - Copia respuesta de la tutela - Copia fallo de la tutela - Solicitud de la tutela - Copia incidente de desacato - Copia respuesta incidente de desacato - Copia impugnación de tutela	Pensionados, Ex trabajadores o Beneficiarios	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión de Prestaciones Económicas	Gestión de Prestaciones Económicas	PÚBLICA CLASIFICADA o USO INTERNO	DATO SENSIBLE	Medio	Medio	Medio
ACTIVO DE INFORMACION	Informes a Otras Entidades	El detalle de la información referente al activo es la siguiente: - Informe estadístico pensiones min-protección	Ministerio de Salud y la Protección Social	No	Español	Análogo o digital	Puf	Disponible	No Publicada	Gestión de Prestaciones Económicas	Gestión de Prestaciones Económicas	PÚBLICA	DATO PÚBLICO	Bajo	Medio	Medio

Cuadro 17. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	EXPEDIENTES PENSIONADOS	El detalle de la información referente al activo es la siguiente: documentación relacionado con la historia pensional - subserie documental que contiene la siguiente documentación: Factura o certificado cancelación de servicio funerario - Certificado de historia laboral - Certificados factores salariales - Copia edicto emplazatorio - Fotocopia documentos de identidad - Registro civil de nacimiento - Solicitud de recurso de reposición - Copia de aceptación de acogimiento - Formulario de afiliación a EPS - Oficio requiriendo documentos - Primera copia de la sentencia - Solicitud de auxilio funerario - Solicitud certificado pensión - Solicitud de reajustes - Solicitud embargo - Oficio informando no aplicación de embargo - Oficio informando reducción de descuentos por embargo - Solicitud mesadas a herederos - Solicitud re liquidación o indexación - Solicitud pensión (vejez, jubilación, sanción) - Liquidación de la pensión - Distribución de cuotas partes - Solicitud consulta cuota parte - Solicitud pago de sentencia pensión - Solicitud acogimiento ley 1204/2008 - Solicitud pago de mesadas - Liquidación mesadas causadas - Copia solicitud de la tutela - Copia respuesta de la tutela - Copia fallo de la tutela - Solicitud revocatoria de poder - Copia incidente de desacato - Copia respuesta incidente de desacato - Copia impugnación de tutela - Proyecto acto administrativo - Copia de resolución - Declaraciones extra juicio - Certificado de causa de retiro - Auxilio funerario	Pensionados, Ex trabajadores	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión Documental	Gestión de Prestaciones Económicas	PÚBLICA RESERVADA	DATO SENSIBLE	Alto	Alto	Alto

Cuadro 17. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo			B. Atributos del Activo			C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	EXPEDIENTE SUSTITUCION PENSIONAL	El detalle de la información referente al activo es la siguiente: documentación relacionado con la historia pensional - subserie documental que contiene la siguiente documentación - Certificado de estudios - Factura o certificado cancelación de servicio funerario - Registro civil de defunción - Registro civil de matrimonio - Solicitud de sustitución pensional - Certificado de historia laboral - Certificados factores salariales - Copia edicto emplazatorio - Fotocopia documentos de identidad - Registro civil de nacimiento - Solicitud de recurso de reposición - Solicitud de acogimiento - Certificación de valoración de incapacidad laboral - Certificado de mesadas cobradas y/o no pagadas - Copia boletín de pago - Copia de aceptación de acogimiento - Liquidación de mesadas - Oficio requiriendo documentos - Primera copia de la sentencia - Solicitud acrecimiento de pensión - Solicitud de auxilio funerario - Solicitud certificado pensión - Solicitud de reajustes - Solicitud embargo - Oficio informando no aplicación de embargo - Oficio informando reducción de descuentos por embargo - Solicitud mesadas a herederos - Solicitud pago de sentencia sustitución pensional - Solicitud prorroga - Solicitud re liquidación o indexación - Solicitud aviso de prensa - Ejemplar aviso de prensa - Copia solicitud de la tutela - Copia respuesta de la tutela - Copia fallo de la tutela - Solicitud revocatoria de poder - Copia incidente de desacato - Copia respuesta incidente de desacato - Copia impugnación de tutela - Proyecto acto administrativo - Copia de resolución - Declaraciones extra juicio	Pensionados, Extrabajadores	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión Documental	Gestión de Prestaciones Económicas	PÚBLICA RESERVADA	DATO SENSIBLE	Alto	Alto	Alto

Cuadro 17. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	EXPEDIENTES BONOS PENSIONALES	El detalle de la información referente al activo es la siguiente: documentación relacionado con la historia pensional - subserie documental que contiene la siguiente documentación: - Certificados de incapacidad - Registro civil de defunción - Certificado de historia laboral - Certificados factores salariales - Copia edicto emplazatorio - Fotocopia documentos de identidad - Registro civil de nacimiento - Solicitud de recurso de reposición - Liquidación provisional - Oficio aceptando la liquidación - Oficio objetando la emisión del bono - Oficio solicitando aceptación de liquidación - Oficio solicitud emisión - Certificado afiliación al sistema de pensiones - Oficio requiriendo documentos - Copia solicitud de la tutela - Copia respuesta de la tutela - Copia fallo de la tutela - Copia incidente de desacato - Copia respuesta incidente de desacato - Copia impugnación de tutela - Proyecto acto administrativo - Copia de resolución	Pensionados	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión Documental	Gestión de Prestaciones Económicas	PÚBLICA RESERVADA	DATO SENSIBLE	Alto	Alto	Alto
ACTIVO DE INFORMACION	Archivos planos con contabilidad, tesorería y bancos	El detalle de la información referente al activo es la siguiente: Archivos para alimentar bases de datos entre los proceso de tesorería, contabilidad y los bancos	Tesorería, Contabilidad	No	Español	Electrónico	TXT	Disponible	No Publicada		Gestión de Prestaciones Económicas	PÚBLICA RESERVADA	DATO PRIVADO	Alto	Alto	Alto
PERSONAS	Abogados Sustanciadores	El detalle de la información referente al activo es la siguiente: Abogados Sustanciadores los tramites de pensión		Si						Gestión de Prestaciones Económicas	Gestión de Prestaciones Económicas			Medio	Medio	Alto

Cuadro 17. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	EXPEDIENTES CUOTAS PARTES POR PAGAR	El detalle de la información referente al activo es la siguiente: documentación relacionado con la historia pensional - subserie documental que contiene la siguiente documentación: - Certificado de historia laboral - Certificados factores salariales - Copia edicto emplazatorio - Liquidación de la pensión y distribución de cuotas partes - Fotocopia documentos de identidad - Oficio objeción de cuota parte - Oficios de consulta - Registro civil de nacimiento - Oficio requiriendo documentos - Copia solicitud de la tutela - Copia respuesta de la tutela - Copia fallo de la tutela - Copia incidente de desacato - Copia respuesta incidente de desacato - Copia impugnación de tutela - Proyecto acto administrativo - Copia de resolución	Pensionados	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión Documental	Gestión de Prestaciones Económicas	PÚBLICA RESERVADA	DATO SENSIBLE	Alto	Alto	Alto
ACTIVO DE INFORMACION	Archivos planos con contabilidad, tesorería y bancos	El detalle de la información referente al activo es la siguiente: Archivos para alimentar bases de datos entre los proceso de tesorería, contabilidad y los bancos	Tesorería, Contabilidad	No	Español	Electrónico	TXT	Disponible	No Publicada		Gestión de Prestaciones Económicas	PÚBLICA RESERVADA	DATO PRIVADO	Alto	Alto	Alto
PERSONAS	Abogados Sustanciadores	El detalle de la información referente al activo es la siguiente: Abogados Sustanciadores los tramites de pensión		Si						Gestión de Prestaciones Económicas	Gestión de Prestaciones Económicas			Medio	Medio	Alto

Cuadro 17. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	Auditorias Medicas de Puntos de Atención	El detalle de la información referente al activo es la siguiente: Programa Anual de Auditorias , el Cronograma de Visitas de Auditoria y Comité Locales, Informe de Auditoría Trimestral Médicos Especialistas e Interventores, Acta Plan de Mejoramiento Hallazgo de Auditoria y Seguimiento a Planes de Mejoramiento con Contratistas Servicios de Salud	IPS	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión de Servicios de Salud	Gestión de Servicios de Salud	PÚBLICA RESERVADA	DATO PRIVADO	Alto	Alto	Alto
ACTIVO DE INFORMACION	Comité Técnico Científico	El detalle de la información referente al activo es la siguiente: Acta elección representantes usuarios ante Comité, Carta de compromiso integrante Comité y Actas comité técnico científico	Ciudadanos	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión de Servicios de Salud	Gestión de Servicios de Salud	PÚBLICA RESERVADA	DATO PRIVADO	Alto	Alto	Alto
ACTIVO DE INFORMACION	Comité AD-HOC	El detalle de la información referente al activo es la siguiente: - Actas comité Ad-Hoc	Ciudadanos	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión de Servicios de Salud	Gestión de Servicios de Salud	PÚBLICA RESERVADA	DATO PRIVADO	Alto	Alto	Alto
ACTIVO DE INFORMACION	Supervisión de Contratos Prestación de Servicios	El detalle de la información referente al activo es la siguiente: Correspondencia de entre el contratista, copias de contratos	Contratistas	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión de Servicios de Salud	Gestión de Servicios de Salud	PÚBLICA RESERVADA	DATO PRIVADO	Alto	Alto	Alto
ACTIVO DE INFORMACION	Comité de Evaluación	El detalle de la información referente al activo es la siguiente: Actas de comité de evaluación regional y municipal de servicios de salud	Pensionados , Contratistas	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión de Servicios de Salud	Gestión de Servicios de Salud	PÚBLICA RESERVADA	DATO PRIVADO	Alto	Alto	Alto

Cuadro 17. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	Valoraciones Medicas Laboral	El detalle de la información referente al activo es la siguiente: Solicitud de valoración, Historia clínica, Informe de la valoración, Dictamen	Ciudadanos, Contratista	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión de Servicios de Salud	Gestión de Servicios de Salud	PÚBLICA RESERVADA	DATO PRIVADO	Alto	Alto	Alto
ACTIVO DE INFORMACION	Facturas Servicios de Salud	El detalle de la información referente al activo es la siguiente: Facturas por servicio, Facturas por servicio de urgencias, Recobros, Facturas de Reembolsos , Tramites de Reembolso	IPS, Pensionados	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión de Servicios de Salud	Gestión de Servicios de Salud	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Alto	Alto	Alto
ACTIVO DE INFORMACION	Incapacidades	El detalle de la información referente al activo es la siguiente: Oficio remisorio de medico auditor o especialista , certificado de incapacidad , formato de control de incapacidades	IPS, Pensionados	SI	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión de Servicios de Salud	Gestión de Servicios de Salud	PÚBLICA RESERVADA	DATO PRIVADO	Alto	Alto	Alto
ACTIVO DE INFORMACION	Certificaciones servicios de salud	El detalle de la información referente al activo es la siguiente: certificaciones de cumplimiento y servicios	IPS	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión de Servicios de Salud	Gestión de Servicios de Salud	PÚBLICA RESERVADA	DATO PRIVADO	Alto	Alto	Alto
ACTIVO DE INFORMACION	Derechos de Petición	El detalle de la información referente al activo es la siguiente: Solicitudes y respuestas a derechos de petición	Ciudadanos	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión de Servicios de Salud	Gestión de Servicios de Salud	PÚBLICA RESERVADA	DATO PRIVADO	Alto	Alto	Alto

Cuadro 17. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	Quejas y Reclamos de Servicios DE Salud	El detalle de la información referente al activo es la siguiente: Oficio de queja, Oficio de solicitud al contratista Oficios trámites realizados	Ciudadanos , IPS	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión de Servicios de Salud	Gestión de Servicios de Salud	PÚBLICA RESERVADA	DATO PRIVADO	Alto	Alto	Alto
ACTIVO DE INFORMACION	RIPS	El detalle de la información referente al activo es la siguiente: Información en Salud Asistencial, Archivos Planos de RIPS, Procesamiento de Información RIPS	Ciudadanos , IPS	Si	Español	Electrónico	Se encuentra en BD	Disponible	No Publicada	Gestión de Servicios de Salud	Gestión de Servicios de Salud	PÚBLICA RESERVADA	DATO PRIVADO	Alto	Alto	Alto

Cuadro 17. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	Informes Estadísticos Técnicos	El detalle de la información referente al activo es la siguiente: Informes estadístico de Pacientes de Alto Costo, Oportunidad en Consultas, Entregas excepcional de Medicamentos, Indicadores de Calidad	IPS prestadoras de servicios de salud, Cuenta de Alto Costo, Ministerio de salud y la protección social	No	Español	Electrónico	Se encuentra en BD	Disponible	No Publicada	Gestión de Servicios de Salud	Gestión de Servicios de Salud	PÚBLICA	DATO PÚBLICO	Bajo	Medio	Alto
ACTIVO DE INFORMACION	Bases de datos Pacientes de Alto Costo	El detalle de la información referente al activo es la siguiente: Informes Técnicos, Pagina web Alto Costo, Archivos Planos de Pacientes de Alto Costo (VIH, Renales, Cáncer; Enfermedades Huérfanas y Osteoarticulares), Cuenta de Alto Costo	IPS prestadoras de servicios de salud, Cuenta de Alto Costo, Ministerio de salud y la protección social Empresas Contratadas para el procesamiento de datos de RIP, UPC y Nuevas Tecnologías,	Si	Español	Electrónico	Se encuentra en BD	Disponible	No Publicada	Gestión de Servicios de Salud	Gestión de Servicios de Salud	PÚBLICA RESERVADA	DATO PRIVADO	Alto	Alto	Alto

Cuadro 17. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	Basa de datos Programa de Promoción y Prevención (Detección Temprana y Protección Específica)	El detalle de la información referente al activo es la siguiente: Resolución 4505, Caracterización Poblacional, Procesamiento de Información de la Resolución 4505, Archivos Planos de la Resolución 4505	IPS prestadoras de servicios de salud, Afiliados a la administrador de plan de beneficios, Entidad contratada para procesamiento de la Resolución 4505 y Ministerio de Salud y la Protección Social	No	Español	Electrónico	Se encuentra en BD	Disponible	No Publicada	Gestión de Servicios de Salud	Gestión de Servicios de Salud	PÚBLICA RESERVADA	DATO PRIVADO	Alto	Alto	Alto
ACTIVO DE INFORMACION	Programa de Promoción y Prevención (Detección Temprana y Protección Específica)	estadísticos 4505 programas caracterización	IPS prestadoras de servicios de salud, Afiliados a la administrador de plan de beneficios, Entidad contratada para procesamiento de la Resolución 4505 y Ministerio de Salud y la Protección Social	No	Español	Electrónico	XLS	Disponible	No Disponible	Gestión de Servicios de Salud	Gestión de Servicios de Salud	PÚBLICA	DATO PÚBLICO	Bajo	Medio	Medio
ACTIVO DE INFORMACION	Bases de datos de Indicadores de Calidad	El detalle de la información referente al activo es la siguiente: Circular única - Circular 057	IPS prestadoras de servicios de salud, Afiliados a la administrador de plan de beneficios, Súper intendencia Nacional de Salud	Si	Español	Electrónico	XLS	Disponible	No Publicada	Gestión de Servicios de Salud	Gestión de Servicios de Salud	PÚBLICA RESERVADA	DATO PÚBLICO	Bajo	Bajo	Medio
ACTIVO DE INFORMACION	Indicadores de Calidad	El detalle de la información referente al activo es la siguiente: Datos estadísticos de portafolio de servicios de circular única	IPS prestadoras de servicios de salud, Afiliados a la administrador de plan de beneficios, Súper intendencia Nacional de Salud	No	Español	Electrónico	XLS	Disponible	Publicada	Gestión de Servicios de Salud	Gestión de Servicios de Salud	PÚBLICA	DATO PÚBLICO	Bajo	Medio	Medio

Cuadro 17. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVOS DE SOFTWARE	DINAMICA GERENCIAL	Módulo de afiliaciones, Planillas Integradas de liquidación de Aportes, Modulo de compensación	Pensionados, Empresas Aportantes	Si	Español	Electrónico	Se encuentra en BD	Disponible	No Publicada	Gestión de TICS	Afiliaciones y Compensación	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Alto	Alto	Bajo
ACTIVO DE INFORMACION	Demandas	El detalle de la información referente al activo es la siguiente: Contestación de Demandas; Fichas Técnicas; actas del Comité de Defensa, Conciliaciones; fallos; Informes del Comité de Defensa Judicial y Conciliación; Actos administrativos para pago de sentencias; Actuaciones en las acciones constitucionales y legales. Representación de la Entidad conferida por el Representante Legal. Actuaciones en las demandas contra el FPS o de éste como demandante. Informes mensuales sobre el estado de los procesos de los apoderados externos.	Integrantes del Comité de Defensa Judicial y conciliación; Grupo Interno de Trabajo de Contabilidad; Gestión Prestaciones Económicas y Archivo Laboral del FPS.	Si	Español	Análogo o digital	Pdf	Disponible	No Publicada	Gestión Documental	Asistencia Jurídica	PÚBLICA RESERVADA	DATO SEMIPRIVADO	Medio	Medio	Alto
ACTIVO DE INFORMACION	Derecho de Petición	El detalle de la información referente al activo es la siguiente: Solicitudes y respuestas a derechos de petición	Todos los procesos, Ciudadanos y partes interesadas	Si	Español	Análogo o digital	Pdf	Disponible	No Publicada	Gestión Documental	Asistencia Jurídica	PÚBLICA	DATO PÚBLICO	Bajo	Bajo	Bajo
ACTIVO DE INFORMACION	Conceptos jurídicos y actos administrativos	El detalle de la información referente al activo es la siguiente: Solicitudes y respuestas a conceptos jurídicos y actos administrativos	Todos los procesos, Ciudadanos y partes interesadas	SI	Español	Análogo o digital	Pdf	Disponible	No Publicada	Gestión Documental	Asistencia Jurídica	PÚBLICA	DATO PÚBLICO	Bajo	Bajo	Bajo

Cuadro 17. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	Estudios Previos	El detalle de la información referente al activo es la siguiente: Actas de aprobación del comité de contratación y estudios previos aprobados	Todos los procesos	No	Español	Análogo o digital	Pdf	Disponible	Publicada	Gestión Tic´s	Asistencia Jurídica	PÚBLICA	DATO PÚBLICO	Bajo	Bajo	Bajo
ACTIVO DE INFORMACION	Elaboración De Pliegos De Condiciones, Ejecución Del Cronograma Del Proceso De Selección Y Elaboración De Contratos Según Modalidad De Contratación	El detalle de la información referente al activo es la siguiente: Acta de aprobación del pliego de condiciones; Resolución de apertura; Contestación a observaciones pliegos; Adendas; Resolución de adjudicación; Contrato, Oficio Remisorio o de Aceptación; Solicitud de Registro Presupuestal; Informe contratación celebrada en el mes inmediatamente anterior; Informe de la gestión contractual	Todos los procesos	No	Español	Análogo o digital	Pdf	Disponible	Publicada	Gestión Tic´s	Asistencia Jurídica	PÚBLICA	DATO PÚBLICO	Bajo	Bajo	Alto
ACTIVO DE INFORMACION	Actuaciones Dentro De Los Procesos De Cobro Coactivo	El detalle de la información referente al activo es la siguiente: Auto avocando o no conocimiento; mandamiento de pago y medidas cautelares; respuesta a excepciones; auto que abre el periodo de prueba; respuesta al recurso de reposición; solicitud de liquidación del crédito; auto de liquidación del crédito y notificación al deudor; auto que resuelve objeciones; embargo; desembargo de excedentes; auto de terminación y archivo del proceso e informe de los deudores que superen los 6 meses y cinco salarios mínimos (boletín de deudores morosos del estado -BDME-.)	Gestión de Recursos Financieros, Deudor, Entidades Bancarias y Contaduría General de la Nación.	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Asistencia Jurídica	Asistencia Jurídica	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Medio	Medio	Bajo

Cuadro 17. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	Actuaciones Dentro De Los Procesos De Cobro Coactivo	El detalle de la información referente al activo es la siguiente: Auto avocando o no conocimiento; mandamiento de pago y medidas cautelares; respuesta a excepciones; auto que abre el periodo de prueba; respuesta al recurso de reposición; solicitud de liquidación del crédito; auto de liquidación del crédito y notificación al deudor; auto que resuelve objeciones; embargo; desembargo de excedentes; auto de terminación y archivo del proceso e informe de los deudores que superen los 6 meses y cinco salarios mínimos (boletín de deudores morosos del estado -BDME-.)	Gestión de Recursos Financieros, Deudor, Entidades Bancarias y Contaduría General de la Nación.	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Asistencia Jurídica	Asistencia Jurídica	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Medio	Medio	Bajo
ACTIVO DE INFORMACION	Liquidación De Contratos	El detalle de la información referente al activo es la siguiente: Actas de liquidación y actos administrativos	Todos los proceso, Contratista	Si	Español	Análogo o digital	Pdf	Disponible	No Publicada	Asistencia Jurídica	Asistencia Jurídica	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Medio	Medio	Alto
ACTIVO DE INFORMACION	Planes Estratégico FPS	Es un documento formulado por la entidad y que se adopta por medio de una acto administrativo, en el cual se reflejan las principales líneas estratégicas a implementar en un periodo determinado de los planes de estratégico, plan de acción, plan anticorrupción y atención al ciudadano	Todos los procesos	No	Español	Electrónico	XLS	Disponible	Publicada	Direccionamiento Estratégico	Direccionamiento Estratégico	PÚBLICA	DATO PÚBLICO	Bajo	Alto	Alto
ACTIVO DE INFORMACION	Resoluciones para el control de documentos	Resoluciones para el control de documentos del Sistema de Gestión de Calidad de la FPS y sus anexos (caracterizaciones de procesos, procedimientos, formatos, instructivos, documentos línea estratégica, fichas técnicas de comités y hojas de vida de Gobierno en Línea)	Todos los procesos	No	Español	Análogo o digital	Pdf	Disponible	Publicada	Direccionamiento Estratégico	Direccionamiento Estratégico	PÚBLICA	DATO PÚBLICO	Bajo	Alto	Alto

Cuadro 17. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	Actas de Comité y Lineamiento Generales	El detalle de la información referente al activo es la siguiente: Citación a comité, Actas comité de gobierno en línea y anti tramites comité de desarrollo admirativo, Documentos soporte del comité	Todos los procesos	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Direccionamiento Estratégico	Direccionamiento Estratégico	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Medio	Medio	Bajo
ACTIVO DE INFORMACION	Informes a Organismos de Control	El detalle de la información referente al activo es la siguiente: Documento mediante el cual se da contestación de una acción de requerimiento de un Organismo de Control	Todos los procesos	No	Español	Análogo o digital	Pdf	Disponible	No Publicada	Direccionamiento Estratégico	Direccionamiento Estratégico	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Medio	Medio	Bajo
ACTIVO DE INFORMACION	Anteproyecto de presupuesto	El detalle de la información referente al activo es la siguiente: Proyección del anteproyecto de presupuesto para la vigencia	Todos los procesos	Si	Español	Análogo o digital	Pdf	Disponible	Publicada	Direccionamiento Estratégico	Direccionamiento Estratégico	PÚBLICA	DATO PÚBLICO	Bajo	Medio	Alto
ACTIVO DE INFORMACION	Documentación Sistema Integral de Gestión	El detalle de la información referente al activo es la siguiente: Instructivos y guías - Planes y programas - Procedimientos - Solicitudes de modificaciones de documentos del SIG - Formatos - Manuales - Códigos - Documentos obsoletos del SIG.	Todos los procesos	No	Español	Análogo o digital	Pdf	Disponible	Publicada	Gestión Tic´s	Direccionamiento Estratégico	PÚBLICA	DATO PÚBLICO	Bajo	Medio	Alto

Cuadro 17. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	Informes de Gestión	El detalle de la información referente al activo es la siguiente: Acta revisión por la dirección - Informe ejecutivo para revisión por la dirección - Informe de gestión anual de FPS - Informe monitoreo de internet - Informes de desempeño de los procesos.	Todos los procesos	No	Español	Analogo o digital	Pdf	Disponible	Publicada	Direccionamiento Estratégico	Direccionamiento Estratégico	PÚBLICA	DATO PÚBLICO	Bajo	Medio	Medio
ACTIVO DE INFORMACION	Informes a Otras Entidades	El detalle de la información referente al activo es la siguiente: Informe a la Cámara de Representantes Comisión Legal de Cuentas - Informe al Congreso de la República Sector de la Protección Social Formulario Único de Reporte de Avance de la Gestión	Cámara de Representantes DAFP -Ministerio de Salud y la Protección Social	No	Español	Analogo o digital	Pdf	Disponible	Publicada	Direccionamiento Estratégico	Direccionamiento Estratégico	PÚBLICA	DATO PÚBLICO	Bajo	Bajo	Bajo
Libros oficiales	Proceso donde se registran todos los movimientos contables de las operaciones realizadas en el Fondo pasivo social se encuentra en el sistemas SIIF			Si		Analogo o digital	Pdf	Disponible	No Publicada	G.I.T de Contabilidad	G.I.T de Contabilidad	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Alto	Alto	Alto
ACTIVO DE INFORMACION	Plan de Adquisición de Bienes y servicios y Obra Publica	Decreto por el cual se liquida el presupuesto general de nación de la vigencia fiscal (Presupuesto Asignado), Solicitudes de Requerimientos de Bienes y Servicios, ante proyectos del plan de Adquisiciones y Estimaciones de Consumo, SECOP y Pagina Web, Coordinador y Encargada Administrativo GIT Gestión Bienes, Compras y Servicios Administrativos	Ministerio de Hacienda, Colombia Compra Eficiente		Español	Analogo o digital	XLS	Disponible	Publicada	Gestión Bienes, Compras y Servicios Administrativos	Gestión Bienes, Compras y Servicios Administrativos	PÚBLICA	DATO PÚBLICO	Bajo	Alto	Alto

Cuadro 17. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
PERSONAS	Coordinador GIT Gestión Bienes, Compras y Servicios Administrativos	Plan de Adquisición de Bienes y servicios y Obra Pública, Administración y Control de Inventarios, Administración y Control de Servicios Públicos y Telecomunicaciones, Administración de Bienes Muebles e Inmuebles	Todos los procesos	SI	Español	Electrónico			No Publicada	Gestión Bienes, Compras y Servicios Administrativos	Gestión Bienes, Compras y Servicios Administrativos	PÚBLICA RESERVADA	DATO PRIVADO	Alto	Alto	Alto
ACTIVO DE INFORMACION	Administración y Control de Servicios Públicos y Telecomunicaciones	Tramite de Facturas y/o Recibos de Pagos, Soportes de Pagos, Control de Servicios Públicos, Profesional GIT Gestión Bienes, Compras y Servicios Administrativos	Tesorería		Español	Electrónico		Disponible	Publicada	Gestión Bienes, Compras y Servicios Administrativos	Gestión Bienes, Compras y Servicios Administrativos	PÚBLICA	DATO PÚBLICO	Bajo	Bajo	Bajo
ACTIVO DE INFORMACION	Control de Servicios Públicos	Publicación de los consumos de servicios públicos en la Intranet de la Entidad	Gestión de TICS		Español	Electrónico		Disponible	Publicada	Gestión Bienes, Compras y Servicios Administrativos	Gestión Bienes, Compras y Servicios Administrativos	PÚBLICA	DATO PÚBLICO	Bajo	Alto	Medio
ACTIVO DE INFORMACION	Administración cuentas personales Bienes Devolutivos	Asignar elementos devolutivos a cada funcionario de la entidad	Gestión de TICS		Español	Electrónico		Disponible	Publicada	Gestión Bienes, Compras y Servicios Administrativos	Gestión Bienes, Compras y Servicios Administrativos	PÚBLICA	DATO PÚBLICO	Bajo	Medio	Medio
ACTIVO DE INFORMACION	Administración cuentas personales Bienes Devolutivos	Diligenciamiento base de datos de cuentas personales, formato cuentas personales inventario individual	Gestión de TICS		Español	Electrónico		Disponible	Publicada	Gestión Bienes, Compras y Servicios Administrativos	Gestión Bienes, Compras y Servicios Administrativos	PÚBLICA	DATO PÚBLICO	Bajo	Medio	Medio

Cuadro 17. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	Administración cuentas personales Bienes Devolutivos	Reintegro de bienes devolutivos - Actualización de Base de datos y cuenta personal de bienes devolutivos.	Todos los funcionarios		Español	Electrónico		Disponible	Publicada	Gestión Bienes, Compras y Servicios Administrativos	Gestión Bienes, Compras y Servicios Administrativos	PÚBLICA	DATO PÚBLICO	Bajo	Medio	Medio
ACTIVO DE INFORMACION	Administración cuentas personales Bienes Devolutivos	Inventario de cuentas personales - semestral	Gestión de TICS		Español	Electrónico		Disponible	Publicada	Gestión Bienes, Compras y Servicios Administrativos	Gestión Bienes, Compras y Servicios Administrativos	PÚBLICA	DATO PÚBLICO	Bajo	Medio	Medio
PERSONAS	Encargado de Administración Cuentas Personales / GIT Gestión Bienes, Compras y Servicios Administrativos	Conocimiento en el manejo en la administración cuentas personales Bienes Devolutivos	Todos los procesos	SI	Español	Físico - papel			No Publicada	Gestión Bienes, Compras y Servicios Administrativos	Gestión Bienes, Compras y Servicios Administrativos	PÚBLICA	DATO PÚBLICO	Bajo	Alto	Medio
ACTIVO DE INFORMACION	Administración de Bienes Muebles e Inmuebles (Transferidos por los extintos Ferrocarriles Nacionales)	Comercialización, Arrendamiento, Comodatos, Pagos de Impuestos Prediales, SIGA (sistema de Información de Gestión de Activos)	Oficina Asesora Jurídica, Contabilidad, Presupuesto y Tesorería		Español	Físico - papel		Disponible	No Publicada	Gestión Bienes, Compras y Servicios Administrativos	Gestión Bienes, Compras y Servicios Administrativos	PÚBLICA	DATO PÚBLICO	Bajo	Alto	Alto
PERSONAS	Técnico Administrativo GIT Gestión Bienes, Compras y Servicios Administrativos	Administración de Bienes Muebles e Inmuebles (Transferidos por los extintos Ferrocarriles Nacionales)	Oficina Asesora Jurídica, Contabilidad, Presupuesto y Tesorería	SI	Español	Físico - papel			No Publicada	Gestión Bienes, Compras y Servicios Administrativos	Gestión Bienes, Compras y Servicios Administrativos	PÚBLICA	DATO PÚBLICO	Alto	Alto	Medio

Cuadro 17. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	Cuentas de cobro	El detalle de la información referente al activo es la siguiente: Cobros realizados a deudores por concepto de cuotas partes pensionales	Contabilidad - Gestión de prestaciones económicas	Si	Español	Electrónico	Se encuentra en BD	Disponible	No Publicada	Gestión Documental	Gestión Cobro	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Bajo	Medio	Bajo
ACTIVO DE INFORMACION	Acreedores de Cuotas partes	El detalle de la información referente al activo es la siguiente: acreencias por concepto de cuotas partes pensionales	Contabilidad - Gestión de prestaciones económicas	Si	Español	Electrónico	Se encuentra en BD	Disponible	No Publicada	Gestión Documental	Gestión Cobro	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Bajo	Medio	Bajo
ACTIVO DE INFORMACION	Resoluciones	Acto administrativo en el cual se reflejan las decisiones administrativas de la entidad, de carácter particular y concreto	Todos los procesos	Si	Español	Análogo o digital	Papel	Disponible	Parcial	Gestión Documental	Secretaria General	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Medio	Medio	Medio
ACTIVO DE INFORMACION	Actuaciones Disciplinarias	procesos disciplinarios que se adelante contra un funcionario		Si	Español	Físico - papel	Papel	Disponible	No Publicada	Secretaria General	Secretaria General	PÚBLICA RESERVADA	DATO PRIVADO	Alto	Alto	Alto
ACTIVO DE INFORMACION	Nomograma Institucional	Leyes, decretos, circulares, resoluciones que aplican a cada uno de los procesos de la entidad	Todos los procesos	No	Español	Electrónico	Se encuentra en BD	Disponible	Publicada	Gestión Tic´s	Secretaria General	PÚBLICA	DATO PÚBLICO	Bajo	Bajo	Medio

Cuadro 17. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	Informes a Otras Entidades	El detalle de la información referente al activo es la siguiente: Solicitud formal en cumplimiento de las actividades inherentes a la función Documento que compila información requerida por los entes externos de control y vigilancia o quien lo requiera. Evidencia de la solicitud o requerimiento de la información Documentos que soportan y evidencias la información requerida		Si	Español	Físico - papel	Papel	Disponible	No Publicada	Secretaria General	Secretaria General	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Medio	Medio	Bajo
ACTIVO DE INFORMACION	Auditorías internas MECI-Calidad	El detalle de la información referente al activo es la siguiente: Programa Anual de Auditorias, Programas Individual de Auditoria , Informes de Auditoría, Actas de reuniones de ciclos de auditorías internas de calidad, Evaluación de auditores de calidad, Informe de evaluación de auditores, Actas de reuniones de ciclos de auditorías internas de calidad, Lista de verificación, Listado de auditores, Solicitud de acciones correctivas y preventivas	Todos los procesos	No	Español	Físico - papel	DOC - EXCEL	Disponible	Publicada	Seguimiento y Evaluación independiente	Seguimiento y Evaluación independiente	PÚBLICA	DATO PÚBLICO	Bajo	Bajo	Bajo
ACTIVO DE INFORMACION	Informes a Organismos de Control	El detalle de la información referente al activo es la siguiente: Certificado Sistema Único de Gestión e Información Litigiosa del Estado Informe de Software Informe Pormenorizado del Estado de Control Interno (ley 1474) Reporte SUIP Encuesta Avance del MECI Informe Ejecutivo del Sistema de Control Interno Informe del sistema de Control Interno Contable Informe de Austeridad del Gasto	Ministerio de Salud y la Protección Social - Presidencia de la República - Procuraduría - DAFP- Derechos de Autor - Contaduría General de la Republica - Agencia Nacional de Defensa Jurídica del Estado	No	Español	Físico - papel	DOC	Disponible	Publicada	Seguimiento y Evaluación independiente	Seguimiento y Evaluación independiente	PÚBLICA	DATO PÚBLICO	Bajo	Bajo	Bajo

Cuadro 17. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	Informes a Otras Entidades	El detalle de la información referente al activo es la siguiente: Solicitud formal en cumplimiento de las actividades inherentes a la función Documento que compila información requerida por los entes externos de control y vigilancia o quien lo requiera. Evidencia de la solicitud o requerimiento de la información Documentos que soportan y evidencias la información requerida		Si	Español	Físico - papel	Papel	Disponible	No publicada	Subdirección de Prestaciones Sociales	Subdirección de Prestaciones Sociales	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Medio	Bajo	Medio
ACTIVO DE INFORMACION	ACCION DE TUTELA	El detalle de la información referente al activo es la siguiente: Documentación sobre comunicación de acción, contestación, fallos, incidente de desacato - subserie documental que contiene la siguiente documentación: Oficio de respuesta tutela - Copia respuesta de la tutela - Copia fallo de la tutela - Solicitud de la tutela - Copia incidente de desacato - Copia respuesta incidente de desacato - Copia impugnación de tutela	Gestión de Prestaciones Económicas	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Subdirección de Prestaciones Sociales	Subdirección de Prestaciones Sociales	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Medio	Medio	Medio
ACTIVO DE INFORMACION	Informes a Otras Entidades	El detalle de la información referente al activo es la siguiente: Solicitud formal en cumplimiento de las actividades inherentes a la función Documento que compila información requerida por los entes externos de control y vigilancia o quien lo requiera. Evidencia de la solicitud o requerimiento de la información Documentos que soportan y evidencias la información requerida		Si	Español	Físico - papel	Papel	Disponible	No publicada	Subdirección de Prestaciones Sociales	Subdirección de Prestaciones Sociales	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Medio	Bajo	Medio

Cuadro 17. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	Formato de control de servicios informáticos	El detalle de la información referente al activo es la siguiente: Estos documentos reflejan la atención a los requerimientos a nivel de hardware, software, redes y comunicaciones a los funcionarios de la entidad	Todos los procesos	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión Tic´s	Gestión Tic´s	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Bajo	Medio	Bajo
ACTIVO DE INFORMACION	Hoja de vida de equipos informáticos	El detalle de la información referente al activo es la siguiente: Documento donde se registran las especificaciones de hardware y software de cada uno de los equipos de la entidad	Todos los procesos	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión Tic´s	Gestión Tic´s	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Medio	Medio	Bajo
ACTIVO DE INFORMACION	Formato de distribución equipos nuevos	El detalle de la información referente al activo es la siguiente: Documentos de carácter administrativo que refleja a quienes se ha sido designado un equipo nuevo dentro de la entidad	Todos los procesos	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión Tic´s	Gestión Tic´s	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Medio	Medio	Bajo
ACTIVO DE INFORMACION	Formato control de ingreso al cuarto de servidores	El detalle de la información referente al activo es la siguiente: Información de control de la entrada y salida del centro de datos		Si	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión Tic´s	Gestión Tic´s	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Medio	Medio	Bajo
ACTIVO DE INFORMACION	Formato creación, modificación y eliminación de usuarios	El detalle de la información referente al activo es la siguiente: Documentos que reflejan el acceso a la información sistematizada del FPS	Todos los procesos	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión Tic´s	Gestión Tic´s	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Medio	Medio	Bajo

Cuadro 17. (Continuación)

ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	
VERSIÓN: 1.0	CÓDIGO:	FECHA ACTUALIZACIÓN:

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	Formato salida de Circulación equipo de computo	El detalle de la información referente al activo es la siguiente: Documentación de los equipos que han salido de circulación de la entidad	Todos los procesos	Si	Español	Físico - papel	Papel	Disponible	No Publicada	Gestión Tic´s	Gestión Tic´s	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Medio	Medio	Bajo
ACTIVO DE INFORMACION	Medios magnéticos	El detalle de la información referente al activo es la siguiente: Cintas magnéticas donde se respalda la información del FPS	Todos los procesos	Si	Español	Electrónico	Se encuentra en BD	Disponible	No Publicada	Gestión Tic´s	Gestión Tic´s	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Medio	Medio	Alto
ACTIVO DE INFORMACION	Servidores de bases de datos de producción	El detalle de la información referente al activo es la siguiente: Servidores de producción que soportan los motores e instancias de bases de datos, maneja todas las solicitudes de acceso a la base de datos ya sea para agregar y eliminar archivos, recuperar y almacenar datos de la aplicaciones dinámica, Safix, Orfeo	Gestión Documental, Gestión de prestaciones económicas , Gestión de Servicios de Salud	Si	Español	Electrónico	Se encuentra en BD	Disponible	No Publicada	Gestión Tic´s	Gestión Tic´s	PÚBLICA RESERVADA	DATO SENSIBLE	Alto	Alto	Alto
SERVICIOS	Portal Web	El detalle de la información referente al activo es la siguiente: Documentación, servicios y contenido de la página institucional	Todos los procesos		Español	Electrónico	Se encuentra en BD	Disponible	publicada	Gestión Tic´s	Gestión Tic´s	PÚBLICA	DATO PÚBLICO	Bajo	Medio	Alto
SERVICIOS	Correo electrónico	El detalle de la información referente al activo es la siguiente: Servidor de Correo Institucional e interno	Todos los procesos	Si	Español	Electrónico	Se encuentra en BD	Disponible	No Publicada	Gestión Tic´s	Gestión Tic´s	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Medio	Medio	Alto

Cuadro 17. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	Intranet	El detalle de la información referente al activo es la siguiente: Documentación del Sistema Integrado de Gestión	Todos los procesos		Español	Electrónico	Se encuentra en BD	Disponible	Publicada	Gestión Tic´s	Gestión Tic´s	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Medio	Medio	Medio
ACTIVO DE INFORMACION	Historial laboral de Personal	El detalle de la información referente al activo es la siguiente: - Acta de posesión - Actas de concurso - Afiliación a cooperativas - Afiliación a otros seguros - Certificado aptitud física - Certificado de antecedentes disciplinarios - Certificado de estudios - Certificado judicial - Certificados de incapacidad - Declaración juramentada de bienes - Embargos judiciales - Evaluación de desempeño - Formato de afiliación a caja de compensación - Formato de afiliación a seguridad social - Formato revisión hojas de vida - Formato único hoja de vida - Fotocopia cedula - Fotocopia libreta militar - Libranzas - Resolución aceptación renuncia - Resolución de inscripción carrera administrativa - Resolución de insubsistencia - Resolución concede turno de vacaciones - Resolución horas extras - Resolución nombramiento - Resolución traslado- Tarjeta profesional- Liquidación de cesantías - Certificado para bonos pensionales - Certificados de tiempo de servicios y funciones - Autorizaciones descuentos por nomina	Sistema de Información y Gestión del Empleo Público -SIGEP Procuraduría General de la Nación Contraloría General de la República	Si	Español	Análogo o digital	Pdf	Disponible	Publicada	Gestión Documental	Gestión de Talento Humano	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Alto	Alto	Alto
ACTIVO DE INFORMACION	Actas Comité Paritario de Salud Ocupacional	El detalle de la información referente al activo es la siguiente: Citación a comité - Actas comité paritario de salud ocupacional - Documentos soporte del comité	Ministerio de Trabajo Aseguradora de Riesgos Laborales	Si	Español	Análogo o digital	Pdf	Disponible en los documentos del proceso GTH según TRD	No Publicada	Gestión Documental	Gestión de Talento Humano	PÚBLICA RESERVADA	datos sensibles	Medio	Alto	Medio

Cuadro 17. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	Programas de Capacitación	El detalle de la información referente al activo es la siguiente: Diagnostico de necesidades - Evaluación a la inducción general - Inducción y re inducción general - Informes de consolidación y análisis de resultados de las encuestas aplicadas - Informes de ejecución y evaluación de los planes - Lista de asistencia a eventos - Evaluación a la inducción especifica - Planes de formación y entrenamiento y de bienestar social - Proyecto PIC - Planes de capacitación PIC -	Página web e intranet FPS Todos los procesos de la entidad	Si	Español	Análogo o digital	Pdf	Disponible en los documentos del proceso GTH según TRD	Disponible en la Página web e intranet FPS	Gestión Documental	Gestión de Talento Humano	PÚBLICA	DATO PÚBLICO	Bajo	Alto	Alto
ACTIVO DE INFORMACION	Actas de Comisión de Personal	El detalle de la información referente al activo es la siguiente: Actas comisión de personal - Documentos soporte gestión comisión personal - Convocatoria comisión de personal	Comisión Nacional del Servicio Civil	Si en algunas ocasiones, cuando se trata temas relacionados con algún funcionario (EDL)	Español	Documento Físico - Medio Electrónico	Documento de texto en TRD-GTH	NO	No Publicada	Gestión Documental	Gestión de Talento Humano	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Medio	Alto	Alto
ACTIVO DE INFORMACION	Actas de Comité de Convivencia Laboral	El detalle de la información referente al activo es la siguiente: Citación- Informes comité de convivencia laboral - Tramite quejas presunto acoso laboral - Actas comité convivencia laboral	Procuraduría General de la Nación	Si	Español	Físico - papel	Documento de texto en TRD-GTH	Disponible en los documentos del proceso GTH según TRD	No Publicada	Gestión Documental	Gestión de Talento Humano	PÚBLICA RESERVADA	DATO SENSIBLE	alto	Alto	Alto

Cuadro 17. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	Certificaciones	El detalle de la información referente al activo es la siguiente: Certificaciones para Bono Pensional de Ex trabajadores y Certificaciones Laborales y de Funciones - Solicitudes - Certificación de información - Oficio remisorio de información	Funcionarios, Todos los procesos, ex trabajadores, Ministerio de Hacienda cooperativas entidades financieras	Si	Español	Analogo o digital	Documento de texto en TRD-GTH	Disponible	No Publicada	Gestión Documental	Gestión de Talento Humano	PÚBLICA RESERVADA	DATO SEMIPRIVADO	Medio	Alto	Alto
ACTIVO DE INFORMACION	Nómina de Funcionarios	El detalle de la información referente al activo es la siguiente: Listado de pago-desprendibles de pago - Novedades de personal - Resumen del pago mensual - Informe de cesantías (reporte) - Solicitud de CDP y RP de nómina y parafiscales - Reporte de libranza y descuento - Resumen de parafiscales - Planilla \"pila\" y autoliquidaciones - Soportes retefuente - Soportes novedades aplicadas - Novedades nomina	software XENCO SAFIX - modulo gestión de nómina Herramientas web (Mi planilla Compensar- SIGEP- FNA) Funcionarios de la entidad	Si	Español	Analogo y digital	Documento de texto y reportes	Disponible	No Publicada	Gestión Documental	Gestión de Talento Humano	PÚBLICA RESERVADA	DATO SEMIPRIVADO	Alto	Alto	Alto
ACTIVO DE INFORMACION	Módulo SAFIX	El detalle de la información referente al activo es la siguiente: Modulo para el manejo de las novedades de personal y nómina de funcionarios activos	software XENCO SAFIX - modulo gestión de nómina	Si	Español	Electrónico	Se encuentra en BD	Disponible	No Publicada	Gestión Documental	Gestión de Talento Humano	PÚBLICA RESERVADA	DATO SEMIPRIVADO	Alto	Alto	Alto
ACTIVO DE INFORMACION	Supervisión de Contratos	El detalle de la información referente al activo es la siguiente: Designación seguimiento - Certificados de cumplimiento - Documentos soporte ejecución supervisión de los contratos asignados.	Proceso de Jurídica	Si	Español	Documento Físico - Medio Electrónico	Documento de texto en TRD-GTH-PDF	Disponible	No Publicada	Gestión Documental	Gestión de Talento Humano	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Medio	Alto	Alto

Cuadro 17. (Continuación)

ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	Supervisión de Contratos	El detalle de la información referente al activo es la siguiente: Designación seguimiento - Certificados de cumplimiento - Documentos soporte ejecución supervisión de los contratos asignados.	Proceso de Jurídica	Si	Español	Documento Físico - Medio Electrónico	Documento de texto en TRD-GTH-PDF	Disponible	No Publicada	Gestión Documental	Gestión de Talento Humano	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Medio	Alto	Alto
ACTIVO DE INFORMACION	Informes a Otras Entidades	El detalle de la información referente al activo es la siguiente: Requerimientos de información - Comunicaciones Oficiales- Anexos - Respuestas de solicitud de información - Reporte novedades SUIP - Informe a la CNSC - Anteproyecto de Presupuesto - Reportes SIGEP	DAFP- Ministerio de Hacienda - Comisión Nacional del Servicio Civil EPS Aseguradoras de Pensiones públicas y privadas ARL COLPENSIONES UGPP CAJA DE COMPENSACIÓN FAMILIAR Registraduría General de la Nación, Contraloría General de la Nación Presidencia de la Republica	SI	Español	Documento Físico - Medio Electrónico	Documento de texto en TRD-GTH - PDF	Disponible	No Publicada	Gestión Documental	Gestión de Talento Humano	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Medio	Alto	Alto
ACTIVO DE INFORMACION	Planes de Emergencia	El detalle de la información referente al activo es la siguiente: Plan de emergencia -Actas e informes de reuniones de brigadas - Inspecciones de seguridad - Programación y ejecución de actividades - Convocatoria, integración y/o conformación	Ministerio de Trabajo Aseguradora de Riesgos Laborales Todos los procesos de la entidad	No	Español	Análogo o digital	Pdf	Disponible en los documentos del proceso GTH según TRD	Disponible en la Página web e intranet FPS	Gestión Documental	Gestión de Talento Humano	PÚBLICA	DATO PÚBLICO	Bajo	Medio	Alto

Cuadro 17. (Continuación)

ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) INVENTARIO DE ACTIVOS DE INFORMACIÓN	
VERSIÓN: 1.0	CÓDIGO:	FECHA ACTUALIZACIÓN:

A. Información del Activo				B. Atributos del Activo		C. Ubicación y Acceso				D. Propiedad		E. Clasificación de la Información		F. Valoración del Activo de Información		
Tipo de Activo	Nombre del Activo	Descripción	Terceros Asociados	¿El activo contiene datos personales?	Idioma	Medio de Conservación y/o Soporte	Formato	Información Disponible	Información Publicada	Proceso Custodio	Proceso Propietario	Clasificación Ley 1712	Clasificación Ley 1581	Confidencialidad	Integridad	Disponibilidad
ACTIVO DE INFORMACION	Sistema de Gestión de la Seguridad y Salud en el Trabajo	El detalle de la información referente al activo es la siguiente: Diagnóstico de necesidades - Formulación plan de salud ocupacional - Ejecución plan salud ocupacional (listas de asistencia a eventos) - Evaluación ejecución plan salud ocupacional - Informe evaluación ejecución plan salud ocupacional - Diagnostico de necesidades - Sistema de gestión de la seguridad social y salud en el trabajo - Reporte e investigación de incidentes y accidentes de trabajo - Análisis estadísticos de incidentes y accidentes de trabajo - Evaluaciones médicas ocupacionales - Dotación elementos de protección personal y seguimiento - Seguimiento, dotación de elementos de protección personal - Gestión comité paritario salud ocupacional (copaso) - Indicadores de gestión de la seguridad y salud en el trabajo - FORMATO MATRIZ DE PERFIL SOCIODEMOGRÁFICO - historias clínicas ocupacionales	ARL Todos los procesos de la entidad	Si	Español	Análogo o digital	Pdf	Disponible	No Publicada (se pública la informa correspondiente al manual del sistema de seguridad en el trabajo)	Gestión Documental	Gestión de Talento Humano	PÚBLICA CLASIFICADA o USO INTERNO	DATO SENSIBLE	Medio	Alto	Alto
ACTIVO DE INFORMACION	Control de asistencia y permanencia en la jornada laboral	El detalle de la información referente al activo es la siguiente: los formatos de ingreso y salida-formato de control de ausencia laborales - informe trimestral de ausentismo laboral	Software Administrador	Si	Español	Análogo o digital	Excel Word	Disponible en los documentos del proceso GTH según TRD	no publicada	Gestión Documental	Gestión de Talento Humano	PÚBLICA RESERVADA	DATO SENSIBLE	Medio	Alto	alto
ACTIVO DE INFORMACION	Administración Gestión Ética-FPS	El detalle de la información referente al activo es la siguiente: Código de valores y de conducta ética - Encuestas y consolidación de resultados	Página web e intranet FPS Todos los procesos	No	Español	Análogo o digital	Pdf	Disponible en los documentos del proceso GTH según TRD	Disponible en la Página web e intranet FPS	Gestión Documental	Gestión de Talento Humano	PÚBLICA CLASIFICADA o USO INTERNO	DATO SEMIPRIVADO	Medio	Alto	Alto

FUENTE: Autores - Inventario De Activos De Información

ANEXO E. Hoja de Vida Indicadores FPS

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI - CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI - CALIDAD) **FORMATO HOJA DE VIDA DEL INDICADOR**		MINSALUD
VERSIÓN: 7.0	CODIGO: PEMYMOPSFO02	FECHA DE ACTUALIZACIÓN: Septiembre 13 de 2016	PAGINA 1 DE 1

DATOS DEL INDICADOR			
INDICADOR ESTRATEGICO ☑		**INDICADOR POR PROCESO** ☐	
Nombre del Proceso:	Gestión TIC´S	**Tipo de Proceso:**	APOYO
Objetivo del Proceso:	Velar por el correcto funcionamiento de los sistemas y la infraestructura Tics de la entidad		
Nombre del Indicador:	ATAQUES INFORMÁTICOS A LA ENTIDAD.	**Código:**	EGTSXX
Objetivo del indicador (Propósito):	Conocer el número de ataques informáticos que recibe la entidad.		
Objetivo Estratégico *	Mantener un sistema de información en línea confiable para todos los usuarios del FPS y ciudadanos, que permita una retroalimentación constante		
Estrategia*	Actualizar y sostener la plataforma tecnológica y los sistemas de información conforme a los requerimientos de la entidad		
(*) Se diligencia sólo para los indicadores estratégicos.			
Tipo de indicador:	EFICIENCIA		

DATOS DEL PROCESO	
Procesos y/o dependencia que suministra información y datos al indicador:	Gestión TIC´S
Responsable de calcular:	Encargado de la seguridad de la información
Responsable de analizar:	Encargado de la seguridad de la información , Jefe de Oficina Asesora de Planeación y Sistemas / Oficina Asesora de Planeación y Sistemas
Usuarios de la información recolectada y analizada:	Dirección General, Medición y Mejora, Seguimiento y Evaluación Independiente.

DESCRIPCIÓN DEL INDICADOR		
FORMULA PARA CALCULAR EL INDICADOR		**FUENTE DE DATOS**
Numerador	No. de acciones preventivas ejecutadas en el semestre	Herramienta de seguridad (Firewall, PCSECURE, Antivirus, Plataforma de correo)
Denominador	/N° de ataques que recibió la entidad en el semestre que impidieron la prestación de algunos de los servicios que la entidad ofrece a los ciudadanos y empresas	
ESCALA	**FRECUENCIA DE RECOLECCIÓN**	**FRECUENCIA DE REVISIÓN**
Porcentaje	Mensual	Semestral

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI - CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI - CALIDAD) **FORMATO HOJA DE VIDA DEL INDICADOR**		MINSALUD
VERSIÓN: 7.0	CODIGO: PEMYMOPSFO02	FECHA DE ACTUALIZACIÓN: Septiembre 13 de 2016	PAGINA 1 DE 1

DATOS DEL INDICADOR			
INDICADOR ESTRATEGICO ☐		**INDICADOR POR PROCESO** ☑	
Nonbre del Proceso:	Gestión TIC´S	**Tipo de Proceso:**	APOYO
Objetivo del Proceso:	Velar por el correcto funcionamiento de los sistemas y la infraestructura TIC¨s de la entidad		
Nombre del Indicador:	INCIDENTES DE SEGURIDAD DE LA INFORMACION	**Código:**	PGTSXX
Objetivo del indicador (Propósito):	Garantizar la administracion de incidente de seguridad de la informacion en la entidad		
Objetivo Estratégico *			
Estrategía*			
(*) Se diligencia sólo para los indicadores estratégicos.			
Tipo de indicador:	EFICIENCIA		

DATOS DEL PROCESO	
Procesos y/o dependencia que suministra información y datos al indicador:	Todos los procesos
Responsable de calcular:	Encargado de la seguridad de la información
Responsable de analizar:	Encargado de la seguridad de la información , Jefe de Oficina Asesora de Planeación y Sistemas / Oficina Asesora de Planeación y Sistemas
Usuarios de la información recolectada y analizada:	Dirección General, Medición y Mejora, Seguimiento y Evaluación Independiente.

DESCRIPCIÓN DEL INDICADOR		
FORMULA PARA CALCULAR EL INDICADOR		**FUENTE DE DATOS**
Numerador	No. de acciones preventivas ejecutadas en el semestre	Herramienta de seguridad (Firewall, PCSECURE, Antivirus, Plataforma de correo), Notificaciones de los procesos
Denominador	Número total de incidentes notificados (reportados)	
ESCALA	**FRECUENCIA DE RECOLECCIÓN**	**FRECUENCIA DE REVISIÓN**
Porcentaje	Por evento	Semestral

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI - CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI - CALIDAD) **FORMATO HOJA DE VIDA DEL INDICADOR**		MINSALUD
VERSIÓN: 7.0	CODIGO: PEMYMOPSFO02	FECHA DE ACTUALIZACIÓN: Septiembre 13 de 2016	PAGINA 1 DE 1

DATOS DEL INDICADOR			
INDICADOR ESTRATEGICO ☑		**INDICADOR POR PROCESO** ☐	
Nombre del Proceso:	Gestión TIC´S	**Tipo de Proceso:**	APOYO
Objetivo del Proceso:	Velar por el correcto funcionamiento de los sistemas y la infraestructura Tics de la entidad		
Nombre del Indicador:	REVISIONES DE LA SEGURIDAD DE LA INFORMACIÓN	**Código:**	PGTSXX
Objetivo del indicador (Propósito):	Garantizar que se implementa y opera la seguridad de la información de acuerdo a las políticas y procedimientos de la entidad		
Objetivo Estratégico *	Mantener un sistema de información en línea confiable para todos los usuarios del FPS y ciudadanos, que permita una retroalimentación constante		
Estrategia*	Actualizar y sostener la plataforma tecnológica y los sistemas de información conforme a los requerimientos de la entidad		
(*) Se diligencia sólo para los indicadores estratégicos.			
Tipo de indicador:	EFICIENCIA		

DATOS DEL PROCESO	
Procesos y/o dependencia que suministra información y datos al indicador:	Todos los procesos
Responsable de calcular:	Encargado de la seguridad de la información
Responsable de analizar:	Encargado de la seguridad de la información , Jefe de Oficina Asesora de Planeación y Sistemas / Oficina Asesora de Planeación y Sistemas
Usuarios de la información recolectada y analizada:	Dirección General, Medición y Mejora, Seguimiento y Evaluación Independiente.

DESCRIPCIÓN DEL INDICADOR		
FORMULA PARA CALCULAR EL INDICADOR		**FUENTE DE DATOS**
Numerador	Promedio de revisiones de cumplimiento de seguridad de la información sin incumplimientos sustanciales.	Auditorias internas
Denominador		
ESCALA	**FRECUENCIA DE RECOLECCIÓN**	**FRECUENCIA DE REVISIÓN**
Porcentaje	Semestral	Semestral

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI - CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI - CALIDAD) **FORMATO HOJA DE VIDA DEL INDICADOR**		MINSALUD
VERSIÓN: 7.0	CODIGO: PEMYMOPSFO02	FECHA DE ACTUALIZACIÓN: Septiembre 13 de 2016	PAGINA 1 DE 1

DATOS DEL INDICADOR			
INDICADOR ESTRATEGICO ☑		**INDICADOR POR PROCESO** ☐	
Nombre del Proceso:	Gestión TIC´S	**Tipo de Proceso:**	APOYO
Objetivo del Proceso:	Velar por el correcto funcionamiento de los sistemas y la infraestructura Tics de la entidad		
Nombre del Indicador:	SENSIBILIZACION Y TOMA DE CONCIENCIA	**Código:**	PGTSXX
Objetivo del indicador (Propósito):	Establecer la efectividad de un plan de capacitación y sensibilización previamente definido como medio de prevención de incidentes de seguridad		
Objetivo Estratégico *	Mantener un sistema de información en línea confiable para todos los usuarios del FPS y ciudadanos, que permita una retroalimentación constante		
Estrategia*	Actualizar y sostener la plataforma tecnológica y los sistemas de información conforme a los requerimientos de la entidad		
(*) Se diligencia sólo para los indicadores estratégicos.			
Tipo de indicador:	EFECTIVIDAD		
DATOS DEL PROCESO			
Procesos y/o dependencia que suministra información y datos al indicador:	Todos los procesos		
Responsable de calcular:	Encargado de la seguridad de la información		
Responsable de analizar:	Encargado de la seguridad de la información , Jefe de Oficina Asesora de Planeación y Sistemas / Oficina Asesora de Planeación y Sistemas		
Usuarios de la información recolectada y analizada:	Dirección General, Medición y Mejora, Seguimiento y Evaluación Independiente.		

DESCRIPCIÓN DEL INDICADOR		
FORMULA PARA CALCULAR EL INDICADOR		**FUENTE DE DATOS**
Numerador	Número de fallas o no cumplimientos encontrados en las sensibilizaciones programadas o eventos realizados para evaluar el tema	Capacitaciones, actividades, listas de asistencia a eventos
Denominador	Total de Funcionario y/o contratista a capacitar.	
ESCALA	**FRECUENCIA DE RECOLECCIÓN**	**FRECUENCIA DE REVISIÓN**
Porcentaje	Semestral	Semestral

Anexo F. Listado Riesgos, Vulnerabilidades y Amenazas FPS

Cuadro 18. Matriz de valoración de activos y análisis de riesgos de seguridad de la información

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) MATRIZ DE VALORACIÓN DE ACTIVOS Y ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

IDENTIFICACIÓN					ANALISIS					EVALUACIÓN					MONITOREO Y REVISIÓN	
					RIESGO INHERENTE					RIESGO RESIDUAL						
Procesos	Activos de Información	Riesgo	Causa / Amenaza	Vulnerabilidad	Probabilidad	Impacto		Nivel Riesgo	Controles	Probabilidad	Impacto		Nivel Riesgo	Medidas de Respuesta	Controles Anexo ISO 27001:2013	Acciones
TODOS LOS PROCESOS	Todos los Activos Información	Perdida , adulteración o deterioro de la información en medio físico y/o digital	• Condiciones inadecuadas de temperatura o humedad • Fuego • Daños por agua • Corte del suministro eléctrico	• Red energética inestable • Falta de cuidado en la disposición final	3	3	A	ZONA DE RIESGO ALTA	CONTROL: backup, procedimiento. RESPONSABLE: Profesional Especializado FRECUENCIA: No establecida TIPO DE CONTROL: Preventivo NATURALEZA DEL CONTROL: Manual CONTROL DOCUMENTADO: NO CALIFICACIÓN DEL CONTROL: Los controles existen, son efectivos pero no están documentados	1	1	B	ZONA DE RIESGO BAJA	Asumir el Riesgo	A.8.2.3 Manejo de activos A.8.3.2 Disposición de los medios A.8.3.3 Transferencia de medios físicos A.9.3 Responsabilidades de los usuarios A.11.1.4 Protección contra amenazas externas y ambientales A.11.2.2 Servicios de suministro A.11.2.3 Seguridad del cableado	P: Diagnostico general del estado de la gestión documental H: Elaboración del programa de gestión documental V: Implementación del programa de gestión documental A: seguimiento del programa de gestión documental

Cuadro 18. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) MATRIZ DE VALORACIÓN DE ACTIVOS Y ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: / FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

IDENTIFICACIÓN					ANALISIS – RIESGO INHERENTE					EVALUACIÓN – RIESGO RESIDUAL					MONITOREO Y REVISIÓN	
Procesos	Activos de Información	Riesgo	Causa / Amenaza	Vulnerabilidad	Probabilidad	Impacto		Nivel Riesgo	Controles	Probabilidad	Impacto		Nivel Riesgo	Medidas de Respuesta	Controles Anexo ISO 27001:2013	Acciones
TODOS LOS PROCESOS	Todos los Activos Información	Alteración y destrucción de la información en las bases de datos.	• Software Malicioso • Accesos no autorizados a los sistemas • Espionaje remoto • Difusión de software dañino Error de los usuarios Alteración accidental de la información.	• Falta de mecanismos de identificación y autentificación, como la autentificación de usuario • Manipulación de los registros de las bases de datos.	3	4	E	ZONA DE RIESGO EXTREMA	CONTROL: Perfiles de usuario establecidos por el administrado de bases de datos, los procedimientos de APGTSOPSPT06 creación, modificación y eliminación de usuarios en el sistema, APGTSOPSPT07 Mantenimiento de servidor de aplicaciones y base datos RESPONSABLE: administrador de bases de datos FRECUENCIA: por evento TIPO DE CONTROL: manual NATURALEZA DEL CONTROL: Preventivo CONTROL DOCUMENTADO: Si CALIFICACIÓN DEL CONTROL: El control se encuentra documentado pero no es efectivos por no se evidencia dentro los procedimientos el seguimientos que se debe hacer al control.	3	4	E	ZONA DE RIESGO EXTREMA	Reducir el Riesgo, Evitar, Compartir o Transferir el Riesgo	A.6.1. Organización Interna. - A.6.1.1. Roles y responsabilidades para la seguridad de la Información. A.9.2. Gestión de Acceso de Usuarios. - A.9.2.4. Gestión de información de autenticación secreta de usuarios. A.9.2. Gestión de Acceso de Usuarios. - A.9.2.4. Gestión de información de autenticación secreta de usuarios. A.9.3. Responsabilidades de los usuarios. - A.9.3.1.Uso de información autenticación secreta. A.9.4 Control de acceso a sistemas y aplicaciones A.9.4.1 Restricción de acceso Información A.9.4.2 Procedimiento de ingreso seguro A.9.4.3 Sistema de gestión de contraseñas A.9.4.4 Uso de programas utilitarios privilegiados A.11.1. Áreas Seguras. - A.11.1.4. Protección contra amenazas externas y ambientales. A.12.2 Protección contra códigos maliciosos A.12.2.1 Controles contra códigos maliciosos A.12.6. Gestión de vulnerabilidades técnicas. - A.12.6.1. Gestión de las vulnerabilidades técnicas.	P: Revisar los procedimientos de APGTSOPSPT06 creación, modificación y eliminación de usuarios en el sistema, APGTSOPSPT07 Mantenimiento de servidor de aplicaciones y base datos H: Modificar los procedimiento colocando puntos de control V: Aprobación de los procedimiento ante el comité de control interno y calidad A: Socialización de los procedimiento a los funcionarios de la entidad.

Cuadro 18. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) MATRIZ DE VALORACIÓN DE ACTIVOS Y ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: / FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

IDENTIFICACIÓN					ANALISIS					EVALUACIÓN					MONITOREO Y REVISIÓN	
					RIESGO INHERENTE					RIESGO RESIDUAL						
Procesos	Activos de Información	Riesgo	Causa / Amenaza	Vulnerabilidad	Probabilidad	Impacto		Nivel Riesgo	Controles	Probabilidad	Impacto		Nivel Riesgo	Medidas de Respuesta	Controles Anexo ISO 27001:2013	Acciones
TODOS LOS PROCESOS	Todos los Activos Información	No cumplimiento de normas, reglamentos, acuerdos y políticas de seguridad de la información.	Divulgación de la información Denegación de servicio Ataques Informático (ingeniería social, suplantación de identidad,).	• Falta de conciencia acerca de la seguridad • Desconocimiento de las políticas de seguridad de la información y/o sus normas, procedimientos, guías de implementación y estándares.	3	3	A	ZONA DE RIESGO ALTA	CONTROL: Dentro del plan institucional se incluyente temas de seguridad de la información tales como: Políticas de seguridad de la información, Buenas Prácticas en tema de seguridad y los boletines informativo RESPONSABLE: Profesional FRECUENCIA: Mensual TIPO DE CONTROL: Manual NATURALEZA DEL CONTROL: Preventivo CONTROL DOCUMENTADO: Si CALIFICACIÓN DEL CONTROL: El control se encuentra documentado porque se realiza un informe de monitoreo del uso de internet donde se evidencia en donde están accediendo los funcionarios y se reflejan acciones tomadas; ha sido efectivo pero es necesario fortalecer más la toma de conciencia por parte de los función.	2	2	B	ZONA DE RIESGO BAJA	Asumir el Riesgo	A.5 Políticas de seguridad de la información A.5.1 Directrices establecidas por la dirección para la seguridad de la información A.5.1.1 Políticas para la seguridad de la información A.5.1.2 Revisión de las políticas para seguridad de la información A.18 Cumplimiento A.18.1 Cumplimiento de requisitos legales y contractuales A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales A.18.1.4 Privacidad y protección de datos personales A.18.2.2 Cumplimiento con las políticas y normas de seguridad.	P: Cronograma de jornada H: Por medio de miércoles de seguridad. V: Encuesta para medir el impacto generado A: Incluir campaña de contraseñas, escritorio limpio y medios removibles , políticas de seguridad y privacidad de información , el buen uso de los equipos de buenas prácticas de seguridad en el plan institucional.

Cuadro 18. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) MATRIZ DE VALORACIÓN DE ACTIVOS Y ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

IDENTIFICACIÓN					ANALISIS RIESGO INHERENTE					EVALUACIÓN RIESGO RESIDUAL					MONITOREO Y REVISIÓN	
Procesos	Activos de Información	Riesgo	Causa / Amenaza	Vulnerabilidad	Probabilidad	Impacto		Nivel Riesgo	Controles	Probabilidad Probabilidad	Impacto		Nivel Riesgo	Medidas de Respuesta	Controles Anexo ISO 27001:2013	Acciones
GESTION TIC´S	Infraestructura tecnológica	Ataques a la infraestructura tecnológica.	• Software Malicioso • Difusión de software dañino • Denegación de servicio • Ingeniería social (picaresca) • Análisis de tráfico • Acceso no autorizado.	• Provisión de recursos e inversiones en infraestructura inadecuadas • Falta de mecanismos de monitoreo • Arquitectura e infraestructura insegura de la red Falta de Mecanismos para detectar periódicamente vulnerabilidades de seguridad en el funcionamiento de: a) su infraestructura, b) redes, c) sistemas de información, d) aplicaciones y/o e) uso de los servicios.	3	4	E	ZONA DE RIESGO EXTREMA	CONTROL: Firewall, PC SECURE, backup RESPONSABLE: Profesional III FRECUENCIA: Diaria TIPO DE CONTROL: Preventivo NATURALEZA DEL CONTROL: Manual CONTROL DOCUMENTADO: Si CALIFICACIÓN DEL CONTROL: Se tiene estas herramientas pero son herramientas que no generan un valor agregado ya que se tiene un control que puede controlar el ataque o contenerlo.	3	4	E	ZONA DE RIESGO EXTREMA	**Reducir el Riesgo, Evitar, Compartir o Transferir el Riesgo**	A.11.2. Equipos - A.11.2.4. Mantenimiento de equipos - A.12.1. Procedimientos operacionales y responsabilidades - A.12.1.1. Procedimientos de operación documentadas - A.12.1. Procedimientos de operación y responsabilidades documentadas - A.12.6. Gestión de vulnerabilidades técnicas. - A.12.6.1. Gestión de las vulnerabilidades técnicas A.13 Seguridad de las comunicaciones A.13.1 Gestión de la seguridad de las redes. A.13.1.1 Controles de seguridad de las redes A.15.1. Seguridad de la información en las relaciones con los proveedores - A.15.1.1. Política de seguridad de la información para las relaciones con proveedores - A.15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores - A.15.1.3. Cadena de suministro de tecnología de información y comunicación A.15.2. Gestión de la prestación de servicios de proveedores - A.15.2.1. Seguimiento y revisión de los servicios de los proveedores A.16.1. Gestión de incidentes y mejoras en la seguridad de la procedimientos - A.16.1.1. Responsabilidades y procedimientos - A.17.1. Continuidad de seguridad de la información	A.11.2. Equipos - A.11.2.4. Mantenimiento de equipos - A.12.1. Procedimientos operacionales y responsabilidades - A.12.1.1. Procedimientos de operación documentadas - A.12.1. Procedimientos de operación y responsabilidades documentadas - A.12.6. Gestión de vulnerabilidades técnicas.

Cuadro 18. (Continuación)

ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) MATRIZ DE VALORACIÓN DE ACTIVOS Y ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	
VERSIÓN: 1.0	CÓDIGO:	FECHA ACTUALIZACIÓN:

IDENTIFICACIÓN					ANALISIS RIESGO INHERENTE					EVALUACIÓN RIESGO RESIDUAL					MONITOREO Y REVISIÓN	
Procesos	Activos de Información	Riesgo	Causa / Amenaza	Vulnerabilidad	Probabilidad	Impacto		Nivel Riesgo	Controles	Probabilidad Probabilidad	Impacto		Nivel Riesgo	Medidas de Respuesta	Controles Anexo ISO 27001:2013	Acciones
GESTIÓN TIC´S / ASISTENCIA JURÍDICA GESTION BIENES TRANSFERIDOS / GESTION DE SERVICIOS ADMINISTRATIVOS / GESTIÓN DE TALENTO HUMANO	Estudios Previos, Elaboración De Pliegos De Condiciones, Ejecución Del Cronograma Del Proceso De Selección Y Elaboración De Contratos Según Modalidad De Contratación, Legalización De Contratos ,Liquidación De Contratos	No cumplimiento y seguimiento a los acuerdos de confidencialidad en los contratos de soporte y mantenimiento de los sistemas de información	Divulgación de la información Perdida, adulteración y mal uso de la información	No cumplimiento de la suscripción de los acuerdos de confidencialidad a terceros, ausencia de monitoreo de los acuerdos.	2	4	A	ZONA DE RIESGO ALTA	CONTROL: Se tiene dentro de la contratos una cláusula de confidencialidad RESPONSABLE: interventor de contratos FRECUENCIA: TIPO DE CONTROL: Manual NATURALEZA DEL CONTROL: Preventivo CONTROL DOCUMENTADO: Si CALIFICACIÓN DEL CONTROL: El control está documentado y no es efectivo por qué no está haciendo seguimiento.	1	3	M	ZONA DE RIESGO MODERADA	Asumir el Riesgo, Reducir el Riesgo	A.15 Relación con los proveedores A.15.1 Seguridad de la información en las relaciones con los proveedores. A.15.1.1 Política de seguridad de la información para las relaciones con proveedores A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores A.15.1.3 Cadena de suministro de tecnología de información y comunicación A.15.2 Gestión de la prestación de servicios con los proveedores A.15.2.1 Seguimiento y revisión de los servicios de los proveedores A.15.2.2 Gestión de cambios en los servicios de proveedores.	P: Definir y establecer la política e información completa sobre aspectos relevantes para la contratación de servicios H: .Introducir estos aspectos establecidos dentro de los contratos V: Verificar del cumplimiento A: Notificar del seguimiento a través de informe de cumplimiento.
ESTION TIC´S TODOS DE LOS PROCESOS	Todos los Activos Información	Fallas en el proceso de copia de respaldo de los procesos debido a que no se puede acceder al respaldo ni a la recuperación de la información de contingencia afectando Disponibilidad de la información.	• Degradación de los soportes de almacenamiento de la información • Falla del equipo • Mal funcionamiento de equipo.	Almacenamiento sin la debida protección.	3	4	E	ZONA DE RIESGO EXTREMA	CONTROL: Se cuenta con un procedimiento se establecen unas carpetas para cada uno de los procesos y estos todos los jueves de cada semana deben colocar la información de su proceso pero todo este proceso se realiza de manera manual y dificulta la restauración RESPONSABLE: Profesional VIII FRECUENCIA: Semanal TIPO DE CONTROL: Manual NATURALEZA DEL CONTROL: Preventivo CONTROL DOCUMENTADO: Si CALIFICACIÓN DEL CONTROL: El control esta documentados pero no es efectivo.	2	3	M	ZONA DE RIESGO MODERADA	Asumir el Riesgo, Reducir el Riesgo	A.6.1. Organización Interna. - A.6.1.1. Roles y responsabilidades para la seguridad de la Información. A.8.2. Clasificación de la Información. - A.8.2.3. Manejo de Activos. A.8.2. Clasificación de la Información. - A.8.2.3. Manejo de Activos. A.8.3. Manejo de medios. - A.8.3.1. Gestión de medios removibles. A.8.2. Clasificación de la Información. - A.8.2.3. Manejo de Activos. A.8.3. Manejo de medios. - A.8.3.1. Gestión de medios removibles. - A.8.3.2. Disposición de los medios de soporte. A.8.2. Clasificación de la Información. - A.8.2.3. Manejo de Activos. A.8.3. Manejo de medios. - A.8.3.1. Gestión de medios removibles. - A.8.3.2. Disposición de los medios de soporte. - A.8.3.3. Transferencia de medios de físicos. A.12.3. Copias de Respaldo. - A.12.3.1.Respaldo de la información. A.18.2. Revisiones de la seguridad de la información. - A.18.2.2. Cumplimiento con las políticas y normas de seguridad.	P: Definir el alcance del Plan de Continuidad del Negocio de los servicios del Fondo. H: Elaboración de los planes relacionados con el Plan de Continuidad del Negocio de los servicios del Fondo. V: Validación y revisión de los documentos elaborados por parte de la dirección. A: Adquisición y ejecución de lo establecido en los planes relacionados con el Plan de Continuidad del Negocio de los servicios de del Fondo.

Cuadro 18. (Continuación)

ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) MATRIZ DE VALORACIÓN DE ACTIVOS Y ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: / FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

IDENTIFICACIÓN					ANALISIS – RIESGO INHERENTE					EVALUACIÓN – RIESGO RESIDUAL					MONITOREO Y REVISIÓN	
Procesos	Activos de Información	Riesgo	Causa / Amenaza	Vulnerabilidad	Probabilidad	Impacto		Nivel Riesgo	Controles	Probabilidad Probabilidad	Impacto		Nivel Riesgo	Medidas de Respuesta	Controles Anexo ISO 27001:2013	Acciones
TODOS LOS PROCESOS	ORFEO, DINAMICA GERENCIAL, Aplicativo SAFIX, Expedientes pensionados, Expediente sustitución pensional, Expedientes bonos pensionales, Expedientes cuotas partes por pagar, Archivos planos con contabilidad, tesorería y bancos, Actuaciones Disciplinarias , Libros oficiales, Auditorias Médicas de Puntos de Atención , Comité Técnico Científico, Comité AD-HOC, Supervisión de Contratos Prestación de Servicios, Comité de Evaluación, Valoraciones Médicas Laboral, Facturas Servicios de Salud , Incapacidades , Certificaciones servicios de salud ,Derechos de Petición, Quejas y Reclamos de Servicios DE Salud, RIPS, Bases de datos Pacientes de Alto Costo, Basa de datos Programa de Promoción y Prevención (Detección Temprana y Protección Específica), Historial laboral de Personal ,Actas de Comité de Convivencia Laboral, Nómina de Funcionarios , Módulo SAFIX, Administración de base de datos, Requerimientos de Bienes Y servicios, Actuaciones Dentro De Los Procesos De Cobro Coactivo, registro contables ,siiff, defensa judicial.	No obtener información correcta hacia los procesos en el tiempo preciso para la toma de decisiones apropiadas.	• Caída del sistema por agotamiento de recursos • Denegación de servicio Interrupción en los servicios.	• Arquitectura e infraestructura insegura de la red • Falta de mecanismos de monitoreo Ausencia o inadecuado procedimiento de control de cambios • Falta de mantenimiento de equipos.	3	2	M	ZONA DE RIESGO MODERADA	CONTROL: Red de alta velocidad GNAP, UPS, línea alterna de ETB, Firewall RESPONSABLE: Proceso Gestión TIC´S FRECUENCIA: No establecida TIPO DE CONTROL: Preventivo NATURALEZA DEL CONTROL: Automático CONTROL DOCUMENTADO: NO CALIFICACIÓN DEL CONTROL: Los controles existen, son efectivos pero no están documentados.	3	2	M	ZONA DE RIESGO MODERADA	Asumir el Riesgo, Reducir el Riesgo	A.11.1.4. Protección contra amenazas externas y ambientales. A.11.2 Equipos A.11.2.1 Ubicación y protección de los equipos A.11.2.2 Servicios de suministro A.11.2.3 Seguridad del cableado A.11.2.4 Mantenimiento de equipos A.12.1.2 Gestión de cambios A.12.1.3 Gestión de capacidad A.12.2 Protección contra códigos maliciosos. A.12.2.1 Controles contra códigos maliciosos A.13 Seguridad de las comunicaciones A.13.1 Gestión de la seguridad de las redes A.13.1.1 Controles de redes A.13.1.2 Seguridad de los servicios de red A.12.2 Protección contra códigos maliciosos A.12.2.1 Controles contra códigos maliciosos A.12.6. Gestión de vulnerabilidades técnicas. - A.12.6.1. Gestión de las vulnerabilidades técnicas.	P: Diagnostico del estado de la UPS, Red eléctrica y Firewall H: Mantenimiento de las UPS, Red eléctrica y actualización del Firewall V: Pruebas de Funcionamiento y penetración A: Realizar la reposición de la UPS E inclusión de reglas para el Firewall.

Cuadro 18. (Continuación)

ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) MATRIZ DE VALORACIÓN DE ACTIVOS Y ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN		MINSALUD
VERSIÓN: 1.0	CÓDIGO:	FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

IDENTIFICACIÓN					ANALISIS					EVALUACIÓN					MONITOREO Y REVISIÓN	
					RIESGO INHERENTE					RIESGO RESIDUAL						
Procesos	Activos de Información	Riesgo	Causa / Amenaza	Vulnerabilidad	Probabilidad	Impacto		Nivel Riesgo	Controles	Probabilidad Probabilidad	Impacto		Nivel Riesgo	Medidas de Respuesta	Controles Anexo ISO 27001:2013	Acciones
GESTION BIENES TRANSFERIDOS / GESTION DE SERVICIOS ADMINISTRATIVOS	Administración y Control de Inventarios- Cierre de Inventarios	Perdidas de bienes o activos fijos del Fondo de Pasivo Social FNC.	perdida y divulgación de la información	• Procedimiento de seguridad física inadecuada • Falta de protección física de las puertas y ventanas de la edificación • Uso inadecuado o descuido del control físico de acceso físico a las edificaciones y los recintos • Falta de control de los activos que se encuentran fuera de las instalaciones Inadecuado inventario de activos físicos.	2	2	B	ZONA DE RIESGO BAJA	CONTROL: Inventario de activo, cámaras , sistema de vigilancia RESPONSABLE: Coordinador de GESTION BIENES TRANSFERIDOS / GESTION DE SERVICIOS ADMINISTRATIVOS FRECUENCIA: no se tiene TIPO DE CONTROL: Automático NATURALEZA DEL CONTROL: Preventivo CONTROL DOCUMENTADO: no se tiene CALIFICACIÓN DEL CONTROL: No se tiene documentado ha sido efectivo.	2	2	B	ZONA DE RIESGO BAJA	Asumir el Riesgo	A.11.1 Áreas seguras A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles físicos de entrada A.11.1.3 Seguridad de oficinas, recintos e instalaciones A.11.1.4 Protección contra amenazas externas y ambientales A.11.1.5 Trabajo en áreas seguras A.11.1.6 Áreas de despacho y carga A.11.2 Equipos A.11.2.1 Ubicación y protección de los equipos A.11.2.2 Servicios de suministro A.11.2.3 Seguridad del cableado A.11.2.4 Mantenimiento de equipos.	P: Elaborar Inspección de los controles establecidos cámaras software de inventario y sistemas de vigilancia H: Ejecutar el plan para optimizar rendimiento del controles cámaras software de inventario y sistemas de vigilancia. V: Realizar seguimiento del controles cámaras software de inventario y sistemas de vigilancia. . A: Realizar informe de resultados de las mejoras implementadas y su impacto.

Cuadro 18. (Continuación)

ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) MATRIZ DE VALORACIÓN DE ACTIVOS Y ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	
VERSIÓN: 1.0	CÓDIGO:	FECHA ACTUALIZACIÓN:

PAGINA 1 DE 1

IDENTIFICACIÓN					ANALISIS					EVALUACIÓN					MONITOREO Y REVISIÓN	
					RIESGO INHERENTE					RIESGO RESIDUAL						
Procesos	Activos de Información	Riesgo	Causa / Amenaza	Vulnerabilidad	Probabilidad	Impacto		Nivel Riesgo	Controles	Probabilidad Probabilidad	Impacto		Nivel Riesgo	Medidas de Respuesta	Controles Anexo ISO 27001:2013	Acciones
GESTION TIC´S	ORFEO, DOCPLUS, Aplicativo SAFIX, SIIF,DINAMICA GERENCIAL, Bases de datos Pacientes de Alto Costo, Basa de datos Programa de Promoción y Prevención (Detección Temprana y Protección Específica), Administración y Control de Inventarios-Cierre de Inventarios (aplicativos de información)	Acceso no autorizado a los sistemas de información, aplicaciones debido a que políticas de contraseñas no seguras afectando la disponibilidad, integradas y confidencialidad de la información,	• Abuso de privilegios de acceso	• Falta de mecanismos de identificación y autentificación, como la autentificación de usuario • Falta de "terminación de la sesión" cuando se abandona la estación de trabajo Contraseñas no seguras la no debida protección de la contraseña asignada.	3	3	A	ZONA DE RIESGO ALTA	CONTROL: Se tiene establecido dentro de la política de bueno uso y manejo de equipo de cómputos, los servicios institucionales de correo electrónico e internet y un procedimiento de creación, modificación y eliminación de usuarios RESPONSABLE: Profesional FRECUENCIA: No TIPO DE CONTROL: Preventivo NATURALEZA DEL CONTROL: Manual CONTROL DOCUMENTADO: Si CALIFICACIÓN DEL CONTROL: El control esta documentados pero no es efectivo.	3	3	A	ZONA DE RIESGO ALTA	Reducir el Riesgo, Evitar, Compartir o Transferir el Riesgo	A.9 Control de acceso A.9.1 Requisitos del negocio para control de acceso A.9.1.1 Política de control de acceso A.9.1.2 Política sobre el uso de los servicios de red A.9.2 Gestión de acceso de usuarios A.9.2.1 Registro y cancelación del registro de usuarios Control A.9.2.2 Suministro de acceso de usuarios A.9.2.3 Gestión de derechos de acceso privilegiado A.9.2.4 Gestión de información de autenticación secreta de usuarios A.9.2.5 Revisión de los derechos de acceso de usuarios A.9.2.6 Retiro o ajuste de los derechos de acceso A.9.3 Responsabilidades de los usuarios A.9.3.1 Uso de la información de autenticación secreta A.9.4 Control de acceso a sistemas y aplicaciones A.9.4.1 Restricción de acceso Información A.9.4.2 Procedimiento de ingreso seguro A.9.4.3 Sistema de gestión de contraseñas A.9.4.4 Uso de programas utilitarios privilegiados A.9.4.5 Control de acceso a códigos fuente de programas A.10 Criptografía A.10.1 Controles criptográficos A.10.1.2 Gestión de llaves.	P: Cronograma de jornada H: Por medio de miércoles de seguridad. V: Encuesta para medir el impacto generado A: Incluir campaña de contraseñas, escritorio limpio y medios removibles , políticas de seguridad y privacidad de información , el buen uso de los equipos de buenas prácticas de seguridad en el plan institucional.

Cuadro 18. (Continuación)

ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) MATRIZ DE VALORACIÓN DE ACTIVOS Y ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: / FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

IDENTIFICACIÓN					ANALISIS – RIESGO INHERENTE					EVALUACIÓN – RIESGO RESIDUAL					MONITOREO Y REVISIÓN	
Procesos	Activos de Información	Riesgo	Causa / Amenaza	Vulnerabilidad	Probabilidad	Impacto		Nivel Riesgo	Controles	Probabilidad Probabilidad	Impacto		Nivel Riesgo	Medidas de Respuesta	Controles Anexo ISO 27001:2013	Acciones
TODOS LOS PROCESOS	ORFEO, DOCPLUS, Aplicativo SAFIX, SIIF,DINAMICA GERENCIAL, Bases de datos Pacientes de Alto Costo, Basa de datos Programa de Promoción y Prevención (Detección Temprana y Protección Específica), Administración y Control de Inventarios-Cierre de Inventarios.	Uso inapropiado por parte de los funcionarios en el manejo de la información contenida en los sistemas de información del Fondo.	• Navegación imprudente por parte de los empleados • Errores y fallos no intencionados • Uso no previsto Alteración accidental de la información.	Ausencia de políticas de uso correcto de activos de información.	4	3	A	ZONA DE RIESGO ALTA	CONTROL: Dentro del plan institucional se incluyente temas de seguridad de la información tales como: Políticas de seguridad de la información, Buenas Prácticas en tema de seguridad, restricciones de páginas prohibidas o filtros web en el firewall el PCSECURE y parametrización de usuarios RESPONSABLE: Profesional FRECUENCIA: Mensual TIPO DE CONTROL: Manual NATURALEZA DEL CONTROL: Preventivo CONTROL DOCUMENTADO: Si CALIFICACIÓN DEL CONTROL: El control se encuentra documentado porque se realiza un informe de monitoreo del uso de internet donde se evidencia en donde están accediendo los funcionarios y se reflejan acciones tomadas; ha sido efectivo pero es necesario fortalecer más la toma de conciencia por parte de los funcionarios.	3	2	M	DE RIESGO MODERADA	Asumir el Riesgo, Reducir el Riesgo	A.5 Políticas de seguridad de la información A.5.1 Directrices establecidas por la dirección para la seguridad de la información A.5.1.1 Políticas para la seguridad de la información A.5.1.2 Revisión de las políticas para seguridad de la información A.8 Gestión de activos A.8.1 Responsabilidad por los activos A.8.1.1 Inventario de activos A.8.1.2 Propiedad de los activos A.8.1.3 Uso aceptable de los activos A.8.1.4 Devolución de activos A.8.2 Clasificación de la información A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información A.8.2.3 Manejo de activos A.8.3.2 Disposición de los medios A.11.2.8 Equipos de usuario desatendidos A.11.2.9 Política de escritorio limpio y pantalla limpia A.18 Cumplimiento A.18.1 Cumplimiento de requisitos legales y contractuales A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales A.18.1.4 Privacidad y protección de datos personales A.18.2.2 Cumplimiento con las políticas y normas de seguridad.	P: Cronograma de jornada H: Por medio de miércoles de seguridad. V: Encuesta para medir el impacto generado A: Incluir campaña de contraseñas, escritorio limpio y medios removibles , políticas de seguridad y privacidad de información , el buen uso de los equipos de buenas prácticas de seguridad en el plan institucional.

Cuadro 18. (Continuación)

ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) MATRIZ DE VALORACIÓN DE ACTIVOS Y ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: / FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

IDENTIFICACIÓN					ANALISIS – RIESGO INHERENTE					EVALUACIÓN – RIESGO RESIDUAL					MONITOREO Y REVISIÓN	
Procesos	Activos de Información	Riesgo	Causa / Amenaza	Vulnerabilidad	Probabilidad	Impacto		Nivel Riesgo	Controles	Probabilidad Probabilidad	Impacto		Nivel Riesgo	Medidas de Respuesta	Controles Anexo ISO 27001:2013	Acciones
TODOS LOS PROCESOS	ORFEO, DINAMICA GERENCIAL, Aplicativo SAFIX, Expedientes pensionados, Expediente sustitución pensional, Expedientes bonos pensionales, Expedientes cuotas partes por pagar, Archivos planos con contabilidad, tesorería y bancos, Actuaciones Disciplinarias , Libros oficiales, Auditorias Médicas de Puntos de Atención , Comité Técnico Científico, Comité AD-HOC, Supervisión de Contratos Prestación de Servicios, Comité de Evaluación, Valoraciones Médicas Laboral, Facturas Servicios de Salud , Incapacidades , Certificaciones servicios de salud ,Derechos de Petición, Quejas y Reclamos de Servicios DE Salud, RIPS, Bases de datos Pacientes de Alto Costo, Basa de datos Programa de Promoción y Prevención (Detección Temprana y Protección Específica), Historial laboral de Personal ,Actas de Comité de Convivencia Laboral, Nómina de Funcionarios , Módulo SAFIX, Administración de base de datos, Requerimientos de Bienes Y servicios.	Información confidencial o sensible quede en disposición de personas que no tiene la autorización apropiada para obtener acceso.	Suplantación de la identidad del usuario	• Procedimiento de seguridad física inadecuada • Intercambio de información confidencial sin procesos definidos para su resguardo • Falta de políticas para el uso correcto de documentos confidenciales. • Falta de procedimiento formal para la autorización de la información disponible al público • Ausencia de procedimientos para clasificación de información Información confidencial almacenada o enviada sin ser cifrada.	3	3	A	ZONA DE RIESGO ALTA	CONTROL: sistemas de vigilancia y cámaras - PCSECURE RESPONSABLE: Proceso Gestión TIC´S FRECUENCIA: TIPO DE CONTROL: Preventivo NATURALEZA DEL CONTROL: Manual CONTROL DOCUMENTADO: No CALIFICACIÓN DEL CONTROL: No se encuentra documentado.	3	3	A	ZONA DE RIESGO ALTA	Reducir el Riesgo, Evitar, Compartir o Transferir el Riesgo	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información A.8.2.3 Manejo de activos A.10.1 Controles criptográficos A.10.1.1 Política sobre el uso de controles criptográficos A.10.1.2 Gestión de llaves A.11.1 Áreas seguras A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles físicos de entrada A.11.1.3 Seguridad de oficinas, recintos e instalaciones A.11.1.4 Protección contra amenazas externas y ambientales A.11.1.5 Trabajo en áreas seguras A.11.1.6 Áreas de despacho y carga.	P: Elaborar Inspección de los controles establecidos cámaras software de inventario y sistemas de vigilancia H: Ejecutar el plan para optimizar rendimiento del controles cámaras software de inventario y sistemas de vigilancia. V: Realizar seguimiento del controles cámaras software de inventario y sistemas de vigilancia. . A: Realizar informe de resultados de las mejoras implementadas y su impacto.

Cuadro 18. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) MATRIZ DE VALORACIÓN DE ACTIVOS Y ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: / FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

IDENTIFICACIÓN					ANALISIS					EVALUACIÓN					MONITOREO Y REVISIÓN	
					RIESGO INHERENTE					RIESGO RESIDUAL						
Procesos	Activos de Información	Riesgo	Causa / Amenaza	Vulnerabilidad	Probabilidad	Impacto		Nivel Riesgo	Controles	Probabilidad Probabilidad	Impacto		Nivel Riesgo	Medidas de Respuesta	Controles Anexo ISO 27001:2013	Acciones
GESTION TIC´S	Todos los Activos Información	Interrupción total o parcial en la plataforma tecnológica del Fondo, debido a la ausencia de estrategias y/o planes de continuidad de negocio afectando la Disponibilidad de la información.	• Fenómeno símico • Fuego • Destrucción de equipo o medios • Hacker, Cracker.	• Ausencia de un sistema de continuidad de negocio • Ubicación física de los equipos • Ubicación física del centro de cómputo • Políticas no aplicadas o no existencia de seguridad física.	4	5	E	ZONA DE RIESGO EXTREMA	CONTROL: No existe RESPONSABLE: No existe FRECUENCIA: No existe TIPO DE CONTROL: No existe NATURALEZA DEL CONTROL: No existe DOCUMENTADO: No existe CALIFICACIÓN DEL CONTROL: NO EXISTEN	4	5	E	ZONA DE RIESGO EXTREMA	Reducir el Riesgo, Evitar, Compartir o Transferir el Riesgo	A.17.1 Continuidad de seguridad de la información -A.17.1.1Planificación de la continuidad de la seguridad de la información -A.17.1.2 Implementación de la continuidad de la seguridad de la información -A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información A.17.2. Redundancia. - A.17.2.1. Disponibilidad de instalaciones de procesamiento de información.	P: Definir el alcance del Plan de Continuidad del Negocio de los servicios del Fondo. H: Elaboración de los planes relacionados con el Plan de Continuidad del Negocio de los servicios del Fondo. V: Validación y revisión de los documentos elaborados por parte de la dirección. A: Adquisición y ejecución de lo establecido en los planes relacionados con el Plan de Continuidad del Negocio de los servicios de del Fondo.
TODOS LOS PROCESOS	Sistemas de información	Violación de derechos de autor	• Instalación de software no autorizado • Copia fraudulenta de software • Uso de Software falso o copiado.	Ausencia de políticas de uso correcto de activos de información.	3	3	A	ZONA DE RIESGO ALTA	CONTROL: Se tiene un agente que restringe la instalación de software no autorizado (PC SECURE) RESPONSABLE: Profesional FRECUENCIA: TIPO DE CONTROL: Manual NATURALEZA DEL CONTROL: Preventivo CONTROL DOCUMENTADO: No se tiene documentado CALIFICACIÓN DEL CONTROL: el control no se tiene documentado y de igual manera no realiza una verificación en los equipos para verificar la instalación de software ilegal o no autorizado y ver si el control que se tiene está siendo efectivo.	3	3	A	ZONA DE RIESGO ALTA	Reducir el Riesgo, Evitar, Compartir o Transferir el Riesgo	A.12.6.2 Restricciones sobre la instalación de software A.18.1.2 Derechos de propiedad intelectual	P: Establecer reglas para la instalación de software por parte de los funcionarios H: Socializar al interior de la entidad V: verificar el cumplimiento a través de la herramienta de PC SECURE A: Realizar informe de la acciones tomadas.

Cuadro 18. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) MATRIZ DE VALORACIÓN DE ACTIVOS Y ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: / FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

IDENTIFICACIÓN					ANALISIS – RIESGO INHERENTE					EVALUACIÓN – RIESGO RESIDUAL					MONITOREO Y REVISIÓN	
Procesos	Activos de Información	Riesgo	Causa / Amenaza	Vulnerabilidad	Probabilidad	Impacto		Nivel Riesgo	Controles	Probabilidad Probabilidad	Impacto		Nivel Riesgo	Medidas de Respuesta	Controles Anexo ISO 27001:2013	Acciones
GESTION DE SERVICIO SALUD/ GESTION DE PRESTACIONES ECONOMICAS / GESTIÓN DE TALENTO HUMANO / GESTIÓN DOCUMENTAL	EXPEDIENTES PENSIONADOS, EXPEDIENTES CUOTAS PARTES POR PAGAR, EXPEDIENTES BONOS PENSIONALES, ACCION DE TUTELA, Quejas y Reclamos de Servicios DE Salud, Valoraciones Medicas Laboral, derechos de Petición, Historial laboral de Personal.	Sustracción de los expedientes historias laborales de extrabajores y/o pensionados, y de beneficiarios al sistema de salud o documentos para uso mal intencionados.	Divulgación de información sensible	• Procedimiento de seguridad física inadecuada • Falta de protección física de las puertas y ventanas de la edificación • Uso inadecuado o descuido del control físico de acceso físico a las edificaciones y los recintos.	3	3	A	ZONA DE RIESGO ALTA	CONTROL: TRD del proceso, foliación de los expedientes digitalización RESPONSABLE: Profesional FRECUENCIA: Diario TIPO DE CONTROL: Manual NATURALEZA DEL CONTROL: Preventivo CONTROL DOCUMENTADO: documentado CALIFICACIÓN DEL CONTROL:: el control está documentado	1	1	B	ZONA DE RIESGO BAJA	Asumir el Riesgo	A.11.1 Áreas seguras A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles físicos de entrada A.11.1.3 Seguridad de oficinas, recintos e instalaciones A.11.1.4 Protección contra amenazas externas y ambientales A.11.1.5 Trabajo en áreas seguras A.11.1.6 Áreas de despacho y carga	P: Diagnostico general del estado de la gestión documental H: Elaboración del programa de gestión documental V: Implementación del programa de gestión documental A: seguimiento del programa de gestión documental

Cuadro 18. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) MATRIZ DE VALORACIÓN DE ACTIVOS Y ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	MINSALUD
VERSIÓN: 1.0	CÓDIGO: FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

IDENTIFICACIÓN					ANALISIS					EVALUACIÓN					MONITOREO Y REVISIÓN	
					RIESGO INHERENTE					RIESGO RESIDUAL						
Procesos	Activos de Información	Riesgo	Causa / Amenaza	Vulnerabilidad	Probabilidad	Impacto		Nivel Riesgo	Controles	Probabilidad Probabilidad	Impacto		Nivel Riesgo	Medidas de Respuesta	Controles Anexo ISO 27001:2013	Acciones
RECURSOS FINANCIEROS	SIIF, Libros oficiales	Ausencia de protocolos de seguridad de la información financiera.	Robo de recursos financieros Divulgación de información financiera y contable	No cumplimiento y aplicación de políticas del SISTEMA INTEGRADO DE INFORMACION FINANCIERA SIIF NACION.	3	4	E	ZONA DE RIESGO EXTREMA	CONTROL: Protocolos de tramites financieros, protector de cheque, firmas registrada, RESPONSABLE: Subdirector financiero coordinador de grupo interno de tesorería FRECUENCIA: cada vez que exista modificación de las actores o la intervienen TIPO DE CONTROL: Manual NATURALEZA DEL CONTROL: Preventivo CONTROL DOCUMENTADO: Si CALIFICACIÓN DEL CONTROL: está documentado y es efectivo.	1	2	B	ZONA DE RIESGO BAJA	Asumir el Riesgo	A.9.2. Gestión de Acceso de Usuarios. - A.9.2.4. Gestión de información de autenticación secreta de usuarios. A.9.3. Responsabilidades de los usuarios. - A.9.3.1.Uso de información autenticación secreta. A.9.4 Control de acceso a sistemas y aplicaciones A.9.4.1 Restricción de acceso Información A.9.4.2 Procedimiento de ingreso seguro A.9.4.3 Sistema de gestión de contraseñas A.9.4.4 Uso de programas utilitarios privilegiados A.18 Cumplimiento A.18.1 Cumplimiento de requisitos legales y contractuales A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales A.18.1.4 Privacidad y protección de datos personales A.18.2.2 Cumplimiento con las políticas y normas de seguridad.	P: Identificar protocolos existentes para mirar la viabilidad de modificación H: Ejecutar pruebas de efectividad V: Elaboración de informe de evaluación de los protocolos A: Con base en los resultados del informe evaluación de los protocolos determinar eficacia de los protocolos planteadas y estudiar la posibilidad de actualizarlos, modificarlos y/o reemplazarlos.

Cuadro 18. (Continuación)

ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) MATRIZ DE VALORACIÓN DE ACTIVOS Y ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN		MINSALUD
VERSIÓN: 1.0	CÓDIGO:	FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

IDENTIFICACIÓN					ANALISIS					EVALUACIÓN					MONITOREO Y REVISIÓN	
					RIESGO INHERENTE					RIESGO RESIDUAL						
Procesos	Activos de Información	Riesgo	Causa / Amenaza	Vulnerabilidad	Probabilidad	Impacto		Nivel Riesgo	Controles	Probabilidad Probabilidad	Impacto		Nivel Riesgo	Medidas de Respuesta	Controles Anexo ISO 27001:2013	Acciones
GESTION TIC´S / GESTION BIENES TRANSFERIDOS / GESTION DE SERVICIOS ADMINISTRATIVOS	Administración y Control de Inventarios- Cierre de Inventarios.	Obsolescencia de los activos tecnológicos	• Funcionamiento deficiente de equipo • Saturación de sistema • Funcionamiento deficiente de software.	• Inadecuados tiempos de respuesta para servicios de mantenimiento • Ausencia o inadecuado procedimiento de control de cambios • Falta de mantenimiento de equipos.	3	3	A	ZONA DE RIESGO ALTA	CONTROL: S tienen procedimientos como MANTENIMIENTO DE SERVIDOR DE INTRANET, MANTENIMIENTO DE SERVIDOR DE APLICACIONES Y BASE DATOS y un indicador MANTENIMIENTO PREVENTIVO DE EQUIPOS el cual se elabora un programa de mantenimiento preventivo RESPONSABLE: Profesional FRECUENCIA: Semestral TIPO DE CONTROL: Manual NATURALEZA DEL CONTROL: Preventivo CONTROL DOCUMENTADO: Si CALIFICACIÓN DEL CONTROL: El control se encuentra documentado pero no es efectivo porque persisten equipos dentro de entidad muy antiguos y parte no realiza en tiempo programa el mantenimiento y las inspecciones de los equipos.	3	3	A	ZONA DE RIESGO ALTA	Reducir el Riesgo, Evitar, Compartir o Transferir el Riesgo	A.8 Gestión de activos A.8.1 Responsabilidad por los activos A.8.1.1 Inventario de activos A.8.1.2 Propiedad de los activos A.8.1.3 Uso aceptable de los activos A.8.1.4 Devolución de activos A.8.2 Clasificación de la información A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información A.8.2.3 Manejo de activos A.8.3.2 Disposición de los medios A.8.3.3 Transferencia de medios físicos A.11.2 Equipos A.11.2.1 Ubicación y protección de los equipos A.11.2.2 Servicios de suministro A.11.2.3 Seguridad del cableado A.11.2.4 Mantenimiento de equipos 12.1 Procedimientos operacionales y responsabilidades A.12.1.2 Gestión de cambios A.12.1.3 Gestión de capacidad.	P: Contar con un contrato de manteamiento preventivo, correctivo y soporte técnico de los equipos de la entidad. H: Realizar ficha técnica y estudio de mercado para el contrato de mantenimiento y soporte de los equipos de la entidad. V: Realizar ficha, estudio de mercado, estudios previos y validarlo con Contratación para iniciar proceso licitatorio. . A: Adquisición del servicio.

FUENTE: Autores - Matriz De Valoración De Activos Y Análisis De Riesgos De Seguridad De La Información

Anexo G. Procedimientos FPS

TIPO DE SOLICITUD:

ELABORACIÓN	**X**	MODIFICACIÓN	

Tipo de Proceso: AP APOYO

Proceso: APGTS GESTION DE TICS

Procedimiento: APGTSOPSPT INVENTARIO, CLASIFICACIÓN Y ETIQUETADO DE ACTIVOS DE INFORMACIÓN

Responsable del Procedimiento: JEFE DE OFICINA DE PLANEACION Y SISTEMAS

Entorno del procedimiento	
Objetivo:	Determinar los criterios que deben utilizar los responsables de los activos de información para la realización y mantener el inventario, la clasificación y etiquetado de activos de información en la entidad.
Alcance:	Aplica a todos los activos de información de la entidad, el cual Inicia con el conocimiento de los activos de información de los procesos y termina con la clasificación de la información y la actualización de los mismos para la mejora del SGSI
Documentos de consulta:	Internos: Guía para la Gestión y Clasificación de Activos de Información. Modelo de Seguridad de la Información con derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones Guía de instrumentos de gestión de información pública
	Externos:
Relaciones Externas:	
Interrelación de procedimientos:	PROCEDIMIENTO PUBLICACIÓN Y ACTUALIZACIÓN DE INFORMACIÓN EN MEDIOS ELECTRÓNICOS (PAGINA WEB INTRANET) APGTSOPSPT01

	COMITÉ INSTITUCIONAL DE DESARROLLO ADMINISTRATIVO ESDESOPSPT10.
Normatividad:	Ley 1712 de 2014 Ley de transparencia y Acceso a la información pública Ley 1266 de 2008 Ley Habeas Datas Ley 1581 de 2012 Ley de Protección de Datos Personales Artículo 2.1.1.4.4.1 del Decreto 1081 de 2015. NTC ISO/IEC 27001:2013
Definiciones:	**Activo:** Cualquier cosa que tiene valor para la organización NTC-ISO /IEC 27001 **Activo de información:** Es todo aquello que las entidades consideran importante o de alta validez para la misma ya que puede contener importante información como lo puede ser Bases de Datos con usuarios, contraseñas, números de cuentas, etc. **Información:** La definición dada por la ley 1712 del 2014, se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. **Información pública:** Es aquella que puede ser accedida por cualquier persona, incluso por personas o entidades externas a la organización, con o sin vínculos laborales, comerciales, legales, entre otros. **Información pública clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley; Es aquella que puede ser accedida por cualquier persona de la compañía, con o sin consentimiento del dueño del activo de información. **Información pública reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley. **Dato personal:** Es cualquier información vinculada o que pueda asociarse a una o varias personas naturales que, dependiendo de su grado de utilización y acercamiento con la intimidad de las personas podrá ser pública, semiprivada o privada. **Dato personal público**: Son aquellos datos personales que las normas y la Constitución han determinado expresamente como públicos y, para cuya recolección y tratamiento, no es necesaria la autorización del titular de la información. (Ej. Dirección, teléfono, datos contenidos en sentencias judiciales ejecutoriadas, datos sobre el estado civil de las personas, entre otros.) **Dato personal semiprivado:** Son datos que no tienen una naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular, sino a un grupo de personas o a la sociedad en general. Para su tratamiento se requiere la autorización expresa del titular de la información. (Ej. Dato financiero y crediticio). **Dato personal privado:** Es un dato personal que por su naturaleza íntima o reservada solo interesa a su titular y para su tratamiento requiere de su autorización expresa. (Ej. Nivel de escolaridad) **Dato personal sensible**: Es aquel dato personal de especial protección, por cuanto afecta la intimidad del titular y su tratamiento puede generar discriminación. NO puede ser objeto de tratamiento a menos que sea requerido para salvaguardar un interés vital del titular o este se encuentre incapacitado y su

	obtención haya sido autorizada expresamente. (Ej. Origen racial o étnico, orientación política, convicciones religiosas, datos biométricos, relativos a la salud, entre otros.) **Clasificación de la Información:** Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la Entidad. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado. **Propietario de la Información:** Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso. **Custodio:** Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado. **Usuario:** Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información. **Confidencialidad:** Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados. **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos. **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera. **Inventario de activos de información:** Es el ejercicio por medio del cual permite clasificar los activos a los se les debe brindar mayor protección e identificar claramente sus características y roles al interior de un proceso. **Etiquetado de activos de información:** Es el ejercicio por medio del cual se tiene la información caracterizada de acuerdo a los criterios de clasificación de la información**.**

ACTIVIDADES			
No.	**Cargo/ Oficina - Grupo Interno de Trabajo:**	**Actividad**	**Observaciones**
1	Encargado de seguridad de la información / Oficina Asesora de Planeación y Sistemas	Orienta y da las pautas del proceso de inventario de activos de información, a los responsables y custodios de la información, con el objeto de que realicen adecuadamente la identificación o inventario de activos y registros de información. Estas actividades tendrán por objetivo rescatar los siguientes datos: Tipo de Activo, Nombre del Activo, Descripción, Terceros Asociados, ¿El activo contiene datos personales?, Idioma, Medio de Conservación y/o Soporte, Formato, Información Disponible, Información Publicada, Proceso Custodio, Proceso Propietario,	Para realizar el levantamiento de los activos de información se deben tener en cuenta la tablas de retención documental de

		Clasificación de la Información y Valoración del Activo de Información.	cada uno de los procesos
2	Secretario General, Subdirectores, Jefes de Oficina Asesora, Coordinadores de Grupos Internos de trabajo	Registra en el formato APGTSOPSPF INVENTARIO DE ACTIVOS DE INFORMACIÓN los activos que se levantaron.	
3	Secretario General, Subdirectores, Jefes de Oficina Asesora, Coordinadores de Grupos Internos de trabajo	Realiza clasificación de los activos inventariados teniendo en cuenta los siguientes criterios de acuerdo a los niveles aliados con los tipos de información y datos declarados en la ley 1712 del 2014 y en ley 1581 de 2012: Ley 1712 del 2014 INFORMACION PÚBLICA RESERVADA: Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica. INFORMACION PÚBLICA CLASIFICADA: Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario. INFORMACION PÚBLICA: Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad. Ley 1581 de 2012 DATO PÚBLICO: Son aquellos datos personales que las normas y la Constitución han determinado expresamente como públicos	

<table>
<tr><td></td><td></td><td>y, para cuya recolección y tratamiento, no es necesaria la autorización del titular de la información. (Ej. Dirección, teléfono, datos contenidos en sentencias judiciales ejecutoriadas, datos sobre el estado civil de las personas, entre otros.)

DATO SEMIPRIVADO: Son datos que no tienen una naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular, sino a un grupo de personas o a la sociedad en general. Para su tratamiento se requiere la autorización expresa del titular de la información. (Ej. Dato financiero y crediticio).

DATO PRIVADO: Es un dato personal que por su naturaleza íntima o reservada solo interesa a su titular y para su tratamiento requiere de su autorización expresa. (Ej. Nivel de escolaridad)

DATO SENSIBLE: Es aquel dato personal de especial protección, por cuanto afecta la intimidad del titular y su tratamiento puede generar discriminación. NO puede ser objeto de tratamiento a menos que sea requerido para salvaguardar un interés vital del titular o este se encuentre incapacitado y su obtención haya sido autorizada expresamente. (Ej. Origen racial o étnico, orientación política, convicciones religiosas, datos biométricos, relativos a la salud, entre otros.)</td><td></td></tr>
<tr><td>4</td><td>Secretario General, Subdirectores, Jefes de Oficina Asesora, Coordinadores de Grupos Internos de trabajo</td><td>Valora los activos de información de acuerdo a las propiedades de la seguridad de la información (confidencialidad, integridad, disponibilidad) definidas en siguientes criterios:

<table>
<tr><th></th><th>CONFIDENCIALIDAD</th><th>INTEGRIDAD</th><th>DISPONIBILIDAD</th></tr>
<tr><td>ALTA</td><td>El conocimiento o divulgación de la información sin autorización impacta negativamente la entidad a nivel de: -Afectación Imagen a nivel nacional. -Incumplimiento legal a nivel de intervenciones regulatorias - Sanciones de Contraloría, Procuraduría y Fiscalía. -Daños totales de la infraestructura de la entidad - conocimiento o divulgación de información que afecte la defensa y seguridad nacional, La seguridad pública, derechos de la infancia y la adolescencia, La salud pública y la intimidad de la persona</td><td>La pérdida de exactitud y estado completo de la información y métodos de procesamientos impacta negativamente de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.</td><td>La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.</td></tr>
<tr><td>MEDIA</td><td>Sea información pública clasificada, datos semiprivado</td><td>Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.</td><td>La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado</td></tr>
<tr><td>BAJA</td><td>Sea información pública, datos públicos</td><td>Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.</td><td>La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.</td></tr>
</table>

En el caso de que los activos de información en los cuales la valoración de la información en dos (2) o todas las propiedades (confidencialidad, integridad, disponibilidad) como calificada como alta es valorada como crítica y si en los cuales la valoración</td><td></td></tr>
</table>

		de la información es alta en una (1) de por lo menos uno de ellas es de nivel medio o bajo es no crítico.	
5	Encargado de seguridad de la información / Oficina Asesora de Planeación y Sistemas, Secretario General, Subdirectores, Jefes de Oficina Asesora, Coordinadores de Grupos Internos de trabajo	Etiqueta los activos clasificados como INFORMACION PÚBLICA RESERVADA, INFORMACION PUBLICA CLASIFICADA, INFORMACION PÚBLICA utilizando las siguientes etiquetas "**IPR**" para la información pública reservada, "**IPC**" información pública clasificada e "**IPB**" información pública.	
6	Secretario General, Subdirectores, Jefes de Oficina Asesora, Coordinadores de Grupos Internos de trabajo	Envía el formato APGTSOPSPF INVENTARIO DE ACTIVOS DE INFORMACIÓN los activos que se levantaron y etiquetados al por medio de correo electrónico al encargado de seguridad de la información de la Oficina Asesora de Planeación y Sistemas para su consolidación.	
7	Encargado de seguridad de la información / Oficina Asesora de Planeación y Sistemas	Realiza consolidación final del inventario de activos de información en el formato APGTSOPSPF INVENTARIO DE ACTIVOS DE INFORMACIÓN y envía a Secretario General, Subdirectores, Jefes de Oficina Asesora, Coordinadores de Grupos Internos de trabajo para su revisión	
8	Encargado de seguridad de la información / Oficina Asesora de Planeación y Sistemas	Solicita por medio de correo a los responsables del proceso registrar en el APGTSOPSPF ÍNDICE DE INFORMACIÓN CLASIFICADA Y RESERVADA el fundamento constitucional o legal que justifica la clasificación o la reserva, señalando expresamente la norma, artículo, inciso o párrafo que la a amparar, esto con el objeto que la ciudadanía conozca cuáles son los documentos que tienen acceso restringido y facilitar las respuestas a solicitudes de acceso a la información pública reservada o clasificada, conforme a lo establecido en el artículo 2.1.1.4.4.1 del Decreto 1081 de 2015. En caso	

		de ser necesario solicita al Encargado de seguridad de la información capacitación y/o asesoría sobre el diligenciamiento de las ítems y/o campos del índice de información clasificada y reservada	
9	Secretario General, Subdirectores, Jefes de Oficina Asesora, Coordinadores de Grupos Internos de trabajo	Ingresa al archivo "ÍNDICE DE INFORMACIÓN CLASIFICADA Y RESERVADA" y registra las casillas "Fecha de Generación Información", "Objetivo legítimo de la excepción", "Fundamento constitucional o legal", "Fundamento Jurídico de la Excepción", "Excepción total o parcial", "Fecha de la Calificación y Plazo de Clasificación o Reserva", dentro de los cinco días hábiles siguientes al semestre cumplido del formato APGTSOPSPF ÍNDICE DE INFORMACIÓN CLASIFICADA Y RESERVADA (ver Guía de instrumentos de gestión de información pública). Envía correo electrónico al Encargado de seguridad de la información.	
10	Encargado de seguridad de la información / Oficina Asesora de Planeación y Sistemas	Verifica y consolida que los registros estén totalmente diligenciados y envía a la oficina Asesora Jurídica para su VoBo.	
11	Jefe de la oficina Asesora Jurídica	Verifica y estudia el formato APGTSOPSPF ÍNDICE DE INFORMACIÓN CLASIFICADA Y RESERVADA. Envía por correo electrónico al Encargado de seguridad de la información los comentarios o sugerencias con respecto al índice de información clasificada y reservada	
12	Encargado de seguridad de la información / Oficina Asesora de Planeación y Sistemas	Presenta el inventario de activos de información al Comité Institucional de Desarrollo Administrativo para su evaluación y aprobación. PASA AL COMITÉ INSTITUCIONAL DE DESARROLLO ADMINISTRATIVO ESDESOPSPT10 y presenta al jefe de la Oficina Asesora de Planeación para su VoBo	
13	Encargado de seguridad de la información / Oficina Asesora de Planeación y Sistemas	VIENE DEL COMITÉ INSTITUCIONAL DE DESARROLLO ADMINISTRATIVO ESDESOPSPT10. Envía por Intranet el inventario de activos, al administrador de la página Web, para su publicación en la página Web del Fondo. PASA AL PROCEDIMIENTO PUBLICACIÓN Y ACTUALIZACIÓN DE INFORMACIÓN EN MEDIOS ELECTRÓNICOS (PAGINA WEB INTRANET) APGTSOPSPT01	

REGISTROS		
Código	Registro	Oficina - Grupo Interno de Trabajo:
APGTSOPSPF	INVENTARIO DE ACTIVOS DE INFORMACIÓN	
APGTSOPSPF	ÍNDICE DE INFORMACIÓN CLASIFICADA Y RESERVADA	

PUNTOS DE CONTROL				
Nº de actividad	**Descripción del riesgo**	**método de control**	**Frecuencia**	**Responsables**
7	Que levante de manera incorrecta los activos de información	Envía a Secretario General, Subdirectores, Jefes de Oficina Asesora, Coordinadores de Grupos Internos de trabajo para su revisión	Por demanda	Encargado de seguridad de la información / Oficina Asesora de Planeación y Sistemas

CONTROL DE CAMBIOS			
Versión	**Fecha y acto administrativo de aprobación**	**Cambio**	**Nombre del solicitante**
1.0		DOCUMENTO NUEVO	**MAURICIO VILLANEDA JIMENEZ**

CONTROL DE DOCUMENTOS			
Elaborado por: **Roselys Silva C.**	**Cargo:** **PROFESIONAL III**	**Fecha:** AGOSTO 8 DE 2016	**Firma:**
Revisado Técnicamente en OPS:	**Cargo:**	**Fecha:**	**Firma:**

TIPO DE SOLICITUD:

ELABORACIÓN	X	MODIFICACIÓN	

Tipo de Proceso: AP APOYO

Proceso: APGTS GESTION DE TICS

Procedimiento: APGTSOPSPT PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Responsable del Procedimiento: JEFE DE OFICINA DE PLANEACION Y SISTEMAS

Entorno del procedimiento	
Objetivo:	Establecer las pautas ante la ocurrencia de incidentes o la detección de amenazas y/o debilidades que pudiesen comprometer la seguridad de los activos de información de la Entidad.
Alcance:	El procedimiento de Gestión de Incidentes de Seguridad de la Información Inicia con el reporte por parte de cualquier usuario (funcionario, contratista) de la Entidad, en base a un caso de afectación de la información almacenada en equipos de cómputo o sistemas de información, que ocasione la perdida, divulgación o modificación no autorizada de información. Y finaliza con la documentación del detalle técnico de la resolución de incidente de seguridad de la información en la Base de Conocimiento incidente de seguridad de la información y cierre del incidente
Documentos de consulta:	Internos:
	Externos:
Relaciones Externas:	
Interrelación de procedimientos:	Procedimiento APGTSOPSPT03 Soporte técnico a usuarios

Normatividad:	Norma ISO 27001:2013 Ley 1581 de 2012 Norma ISO 27035.
Definiciones:	**Incidente de seguridad de la información:** Según la norma ISO 27035, un Incidente de Seguridad de la Información es indicado por un único o una serie de eventos de seguridad de la información indeseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información. **Evento de seguridad:** Una ocurrencia identificada en el estado de un sistema, servicio o red, indicando una posible violación de la seguridad de la información, política o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad. **Amenaza:** Es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema **Activo de información**: Es todo aquello que las entidades consideran importante o de alta validez para la misma ya que puede contener importante información como lo puede ser Bases de Datos con usuarios, contraseñas, números de cuentas, etc. **Base de conocimiento de incidente de seguridad de la información:** medio por el cual se comparte conocimiento concernientes a resoluciones de incidente de seguridad de la información, con el fin de mejorar la productividad del equipo de atención de incidente de seguridad de la información, debido a que permite reducir significativamente los tiempos de resolución de los i de incidente de seguridad de la información al encontrar respuesta de incidente de seguridad de la información similares

ACTIVIDADES			
No.	**Cargo/ Oficina - Grupo Interno de Trabajo:**	**Actividad**	**Observaciones**
1	Funcionarios / Contratistas /	Reporta la ocurrencia de incidentes o la detección de amenazas y/o debilidades que pudiesen comprometer la seguridad de los activos de información de la entidad mediante el envío de correo electrónico a la siguiente cuenta: seguridadinformacion@fps.gov.co; colocando en el asunto del correo la frase “Incidente de seguridad de información” u otra similar que permita reconocer la situación rápidamente, deberá ser lo más claro y preciso en especificar el incidente o amenaza y a que recursos tecnológicos podría estar	En caso de que el incidente y/o amenaza, requiera de una intervención urgente, se deberá contactar a personal del Proceso Gestión Tic´s vía telefónica o personalmente, sin necesidad de enviar un correo electrónico En el formato APGTSOPSPF REPORTE DE INCIDENTES, AMENAZAS Y/O DEBILIDADES DE SEGURIDAD DE LA INFORMACION se diligencia hasta descripción del incidente

		afectando, anexando el formato APGTSOPSPF REPORTE DE INCIDENTES, AMENAZAS Y/O DEBILIDADES DE SEGURIDAD DE LA INFORMACION	
2	Funcionario encargado de la seguridad de la información	Evalúa para determinar si el caso corresponde a un incidente de seguridad de la Información para realizar el correspondiente escalamiento	
3	Funcionario encargado de la seguridad de la información	Valida si el caso corresponde a un incidente de seguridad. Si la validación es afirmativa, continúa con la actividad 6; de lo contrario continúa pasa al Procedimiento APGTSOPSPT03 Soporte técnico a usuarios	
4	Funcionario encargado de la seguridad de la información	Recolecta información sobre el incidente de seguridad para determinar sus alcance y los sistemas registrando la información en el formato APGTSOPSPF REPORTE DE INCIDENTES, AMENAZAS Y/O DEBILIDADES DE SEGURIDAD DE LA INFORMACION	
5	Funcionario encargado de la seguridad de la información	Determina el tipo de incidente (para ello se presenta un listado de ejemplo en las "observaciones"), establece su criticidad dependiendo del tipo de incidente, naturaleza del activo afectado, cantidad de activos, sistemas o unidades afectadas, impacto en la entidad y de la urgencia en la solución (ver ejemplo en la "las "observaciones del procedimiento") y prioriza los incidentes y su tiempos respuesta de esta manera atenderlos adecuadamente según la necesidad defiendo las siguientes variables:	La severidad del incidente puede ser: Alto Impacto: El incidente de seguridad afecta a activos de información considerados de impacto catastrófico y mayor que influyen directamente a los objetivos misionales de la entidad Se incluyen en esta categoría aquellos incidentes que afecten la reputación y el buen nombre o involucren aspectos legales. Estos incidentes deben tener respuesta inmediata. Medio Impacto: El incidente de seguridad afecta a activos de

Prioridad
Criticidad de impacto
Impacto Actual
Impacto Futuro

Luego de tener definidas las variables se obtiene la prioridad mediante la siguiente fórmula:

Nivel Prioridad = (Impacto actual * 2,5) + (Impacto futuro * 2,5) + (Criticidad del Sistema * 5)

Compara con la siguiente tabla para determinar

la prioridad de atención:

Nivel Prioridad	Valor
Inferior	00,00 – 02,49
Bajo	02,50 – 03,74
Medio	03,75 – 04,99
Alto	05,00 – 07,49
Superior	07,50 – 10,00

información considerados de impacto moderado que influyen directamente a los objetivos de un proceso determinado.

Bajo Impacto: El incidente de seguridad afecta a activos de información considerados de impacto menor e insignificante, que no influyen en ningún objetivo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto

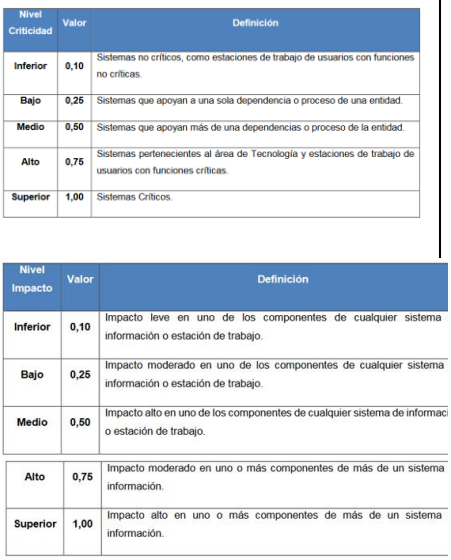
Clasificación De Incidentes De Seguridad De La Información

Acceso no autorizado: Es un incidente que involucra a una persona, sistema o código malicioso que obtiene acceso lógico o físico sin autorización adecuada del dueño a un sistema, aplicación, información o un activo de información.

Modificación de recursos no autorizado: Un incidente que involucra a una persona, sistema o código malicioso que afecta la integridad de la información o de un sistema de procesamiento.

Uso inapropiado de recursos: Un incidente que involucra a una persona que viola alguna política de uso de recursos.

No disponibilidad de los recursos: Un incidente que involucra a una persona, sistema o código malicioso que impide el uso autorizado de un activo de información.

			Multicomponente: Un incidente que involucra más de una categoría anteriormente mencionada. Otros: Un incidente que no puede clasificarse en alguna de las categorías anteriores. Este tipo de incidentes debe monitorearse con el fin de identificar la necesidad de crear nuevas categorías 
6	Funcionario encargado de la seguridad de la información	Registra el Incidente. Si no existe, se registra la notificación y se relevan los datos básicos (fecha y hora de la notificación, propietario de activo, información de contacto, descripción del incidente, sistemas y unidades afectadas)	
7	Funcionario encargado de la seguridad de la información	Informa el Estado; si el Incidente Reportado ya se encuentra registrado y en tratamiento, se informa al Funcionario que lo reportó, indicando el conocimiento del mismo y el estado de la investigación	
8	Funcionario encargado de la seguridad	Analiza la información del incidente accediendo a los logs y registros de información disponible para construir	Dependiendo del tipo de incidente se revisan:

Nivel Criticidad	Valor	Definición
Inferior	0,10	Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas.
Bajo	0,25	Sistemas que apoyan a una sola dependencia o proceso de una entidad.
Medio	0,50	Sistemas que apoyan más de una dependencias o proceso de la entidad.
Alto	0,75	Sistemas pertenecientes al área de Tecnología y estaciones de trabajo de usuarios con funciones críticas.
Superior	1,00	Sistemas Críticos.

Nivel Impacto	Valor	Definición
Inferior	0,10	Impacto leve en uno de los componentes de cualquier sistema información o estación de trabajo.
Bajo	0,25	Impacto moderado en uno de los componentes de cualquier sistema información o estación de trabajo.
Medio	0,50	Impacto alto en uno de los componentes de cualquier sistema de informaci o estación de trabajo.
Alto	0,75	Impacto moderado en uno o más componentes de más de un sistema información.
Superior	1,00	Impacto alto en uno o más componentes de más de un sistema información.

	de la información	una línea de tiempo y determinar la traza de las acciones sucedidas	Logs de acceso de routers y firewalls Logs de intento de login de usuarios Logs de acceso y error de webservers y correo Logs de antivirus Reportes de uso de equipamiento de red
9	Funcionario encargado de la seguridad de la información	Contiene y evita que se propague el incidente. Inmediatamente se determina si el Profesional o Equipo asignado al incidente cuenta con el personal y la experiencia para solucionar el problema en forma definitiva o temporal y en los tiempos apropiados. Si se determina que por alguna causa no lo puede solucionar definitivamente, o si el equipo de incidentes determina que la gravedad del incidente lo amerita, se realiza el escalamiento al proveedor correspondiente	
10	Funcionario encargado de la seguridad de la información	Documenta el detalle técnico de la resolución de incidente de seguridad de la información en la APGTSOPSPF BASE DE CONOCIMIENTO INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN y los cierra.	

REGISTROS		
Código	Registro	Oficina - Grupo Interno de Trabajo:
APGTSOPSPF	BASE DE CONOCIMIENTO DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Oficina Asesora de Planeación y Sistemas
APGTSOPSPF	REPORTE DE INCIDENTES, AMENAZAS Y/O	Oficina Asesora de Planeación y Sistemas

	DEBILIDADES DE SEGURIDAD DE LA INFORMACION	

PUNTOS DE CONTROL				
Nº de actividad	**Descripción del riesgo**	**método de control**	**Frecuencia**	**Responsables**
10	Bases de conocimiento de incidentes de seguridad de la información desactualizada	Documenta el detalle técnico de la resolución de incidente de seguridad de la información en la Base de Conocimiento incidente de seguridad de la información	Por demanda	Funcionario encargado de la seguridad de la información

CONTROL DE CAMBIOS			
Versión	**Fecha y acto administrativo de aprobación**	**Cambio**	**Nombre del solicitante**
1.0		DOCUMENTO NUEVO	**MAURICIO VILLANEDA JIMÉNEZ**

CONTROL DE DOCUMENTOS			
Elaborado por: **Roselys Silva Cuadrado**	**Cargo:** **Profesional**	**Fecha:** AGOSTO /31/2016	**Firma:**
Revisado Técnicamente en OPS:	**Cargo:**	**Fecha:**	**Firma:**
Aprobado Mediante Acta No : Acto Administrativo: Fecha:			

Anexo H. Reconocimiento Vulnerabilidades Fondo Pasivo Social

RECONOCIMIENTO VULNERABILIDADES FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA

Fecha de Vigencia: DD / MM / AA

TABLA DE CONTENIDO

1. OBJETIVO

Identificar y listar las amenazas y vulnerabilidades más relevantes con que cuenta la entidad Fondo de Pasivo Social Ferrocarriles de Colombia con el fin de obtenerlo como insumo para el proyecto de grado denominado: “Diseño Del Modelo De Seguridad Y Privacidad De La Información Basada En Los Requerimientos De La Estrategia De Gobierno En Línea Para La Entidad El Fondo Pasivo Social Ferrocarriles Nacionales De Colombia”.

2. PROCESOS REALIZADOS

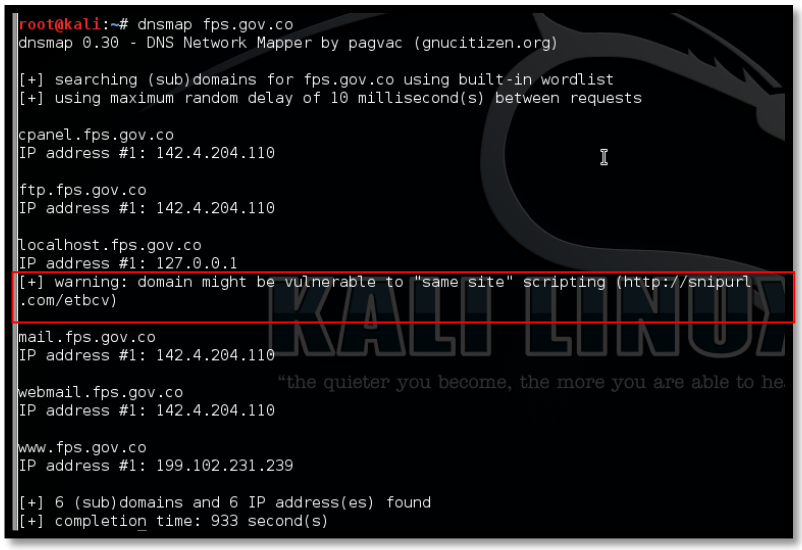
Para el logro de este objetivo, se procedió a utilizar la técnica de evaluación de la NIST SP800-115 basada en la metodología abierta de testeo de seguridad y que permite identificar sistemas, puertos, servicios y vulnerabilidades potenciales mediante el uso de herramientas tecnológicas.

Con previa aprobación del personal del proceso Gestión de TIC´S con el fin de evitar cualquier ilegalidad o conflicto, se realizó lo siguiente:

2.1 SUBDOMINIO/IP

Como primer paso fue la búsqueda de las posibles IP de equipos del dominio de la entidad, esto desde una máquina virtual kali, utilizando la herramienta nmap.
Al utilizar la herramienta se puede evidenciar seis direcciones IP relacionadas con el dominio de la entidad las cuales se ven en la Figura 1:

Figura 1. Búsqueda de direcciones ip



Teniendo en cuenta lo anterior, se identificó que el dominio podría ser vulnerable a secuencias de comandos o Crosssite scripting.

2.2 CUENTAS DE CORREO

Después, se realizó una búsqueda de correos electrónicos de empleados de la entidad, mediante la búsqueda avanzada de Google, con el fin de identificar la estructura para la creación de correos y ver qué tan cuidadosos son al dejar información como esta en la red.
Al utilizar la búsqueda se puede evidenciar lo sé observa en la figura 2, 3, 4, 5, y 6

Figura 2. Búsqueda avanzada de Google

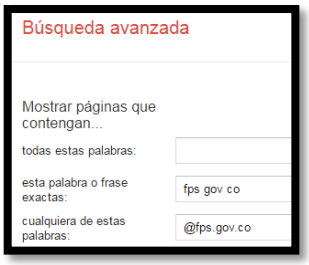


Figura3. Correos encontrados

Figura 4. Correos encontrados

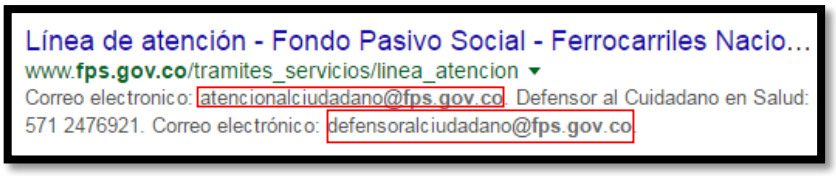
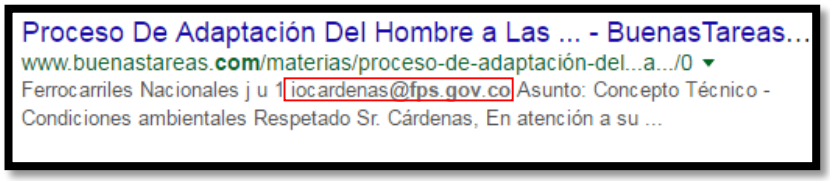


Figura 5. Correos encontrados

Figura 6. Correos encontrados



Se obtuvieron direcciones de interés público como quejasyreclamos@fps.gov.co, atencionalciudadano@fps.gov.co y defensoralciudadano@fps.gov.co, pero adicional a ello, se obtuvieron algunos contactos como: nancybautista@fps.gov.co, Hernando.penaloza@fps.gov.co y iocardenas@fps.gov.co, correos que claramente son de empleados de la entidad y que al estar volando por la red, pueden ser recolectado por bots y hacer que los dueños de este, reciban correos fraudulentos o con software malicioso.

2.3 INFORMACIÓN DE SITIO WEB

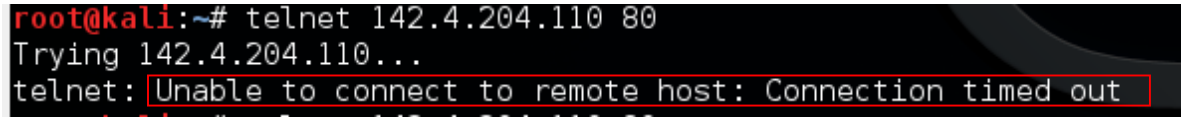
Por medio de la página web Whois, se realizó una búsqueda de información del sitio web, sin embargo se encontró que este dominio se reporta como disponible, véase Figura 7.

Figura 7. Página Whois

2.4 SISTEMA OPERATIVO

Del mismo modo se trató de hacer un reconocimiento al sistema operativo donde está la página web pero no se logró debido a la seguridad que tiene la entidad al respecto como se evidencia en la figura 8.

Figura8. Reconocimiento SO



2.5 ESCANEO DE VULNERABILIDADES

Otra de las herramientas utilizadas fue OWASP ZAP que identificó tres vulnerabilidades del sitio web descritas en la cuadro 19, 20 y 21:

Cuadro 19.Resumen Reporte ZAP

Criticidad	Vulnerabilidad
Low (Medium)	Cross-Domain JavaScript Source File Inclusion
Low (Medium)	Web Browser XSS Protection Not Enabled
Low (Medium)	X-Content-Type-Options Header Missing
Fuentes: Herramientas OWASP ZAP	

Cuadro 20. Resumen de alertas

Risk Level	Number of Alerts
High	0
Medium	0
Low	3
Informational	0

Cuadro 21. Detalle de alertas

Low (Medium)	Cross-Domain JavaScript Source File Inclusion
Description	The page at the following URL includes one or more script files from a third-party domain
URL	http://www.fps.gov.co/
Parameter	http://translate.google.com/translate_a/element.js?cb=googleTranslateElementInit2
Evidence	http://translate.google.com/translate_a/element.js?cb=googleTranslateElementInit2
URL	http://www.fps.gov.co/
Parameter	http://joomla-gtranslate.googlecode.com/svn/trunk/gt_update_notes0.js
Evidence	http://joomla-gtranslate.googlecode.com/svn/trunk/gt_update_notes0.js
URL	http://www.fps.gov.co/cli/
Parameter	http://translate.google.com/translate_a/element.js?cb=googleTranslateElementInit2
Evidence	http://translate.google.com/translate_a/element.js?cb=googleTranslateElementInit2
URL	http://www.fps.gov.co/cli/
Parameter	http://joomla-gtranslate.googlecode.com/svn/trunk/gt_update_notes0.js
Evidence	http://joomla-gtranslate.googlecode.com/svn/trunk/gt_update_notes0.js
Instances	4
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application
Fuente: OWASP ZAP	

Cuadro 21. (Continuación)

Cuadro 21. (Continuación)

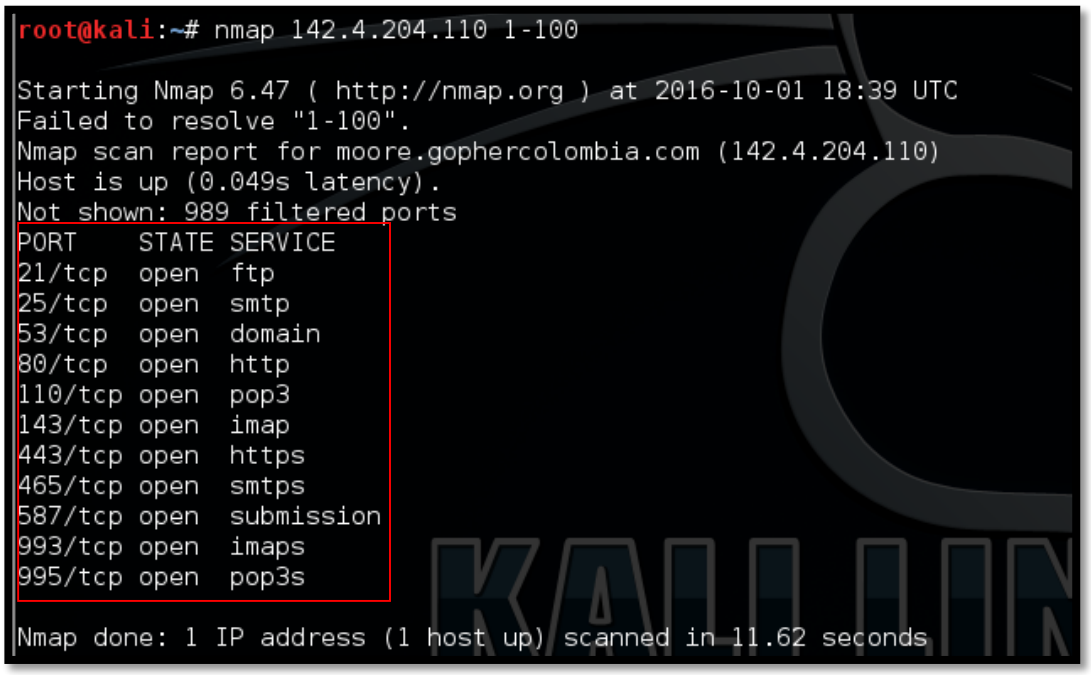
Low (Medium)	Web Browser XSS Protection Not Enabled
Description	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server
URL	http://www.fps.gov.co/
URL	http://www.fps.gov.co/robots.txt
URL	http://www.fps.gov.co/cli/
Instances	3
Solution	Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.
Other information	The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it: X-XSS-Protection: 1; mode=block X-XSS-Protection: 1; report=http://www.example.com/xss The following values would disable it: X-XSS-Protection: 0 The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit). Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).
Reference	https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/
CWE Id	933
WASC Id	14
Fuente: OWASP ZAP	
Low (Medium)	X-Content-Type-Options Header Missing

Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://www.fps.gov.co/
URL	http://www.fps.gov.co/robots.txt
URL	http://www.fps.gov.co/cli/
Instances	3
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Other information	This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scanner will not alert on client or server error responses.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
WASC Id	15
Fuente: OWASP ZAP	

2.6 IDENTIFICACIÓN DE PUERTO Y SERVICIOS

Adicionalmente, se realizó un escaneo de puertos del 1 al 100, encontrando abiertos los puertos que se ven en la Figura 9.

Figura 9. Escaneo Puertos


root@kali:~# nmap 142.4.204.110 1-100
Starting Nmap 6.47 (http://nmap.org) at 2016-10-01 18:39 UTC
Failed to resolve "1-100".
Nmap scan report for moore.gophercolombia.com (142.4.204.110)
Host is up (0.049s latency).
Not shown: 989 filtered ports
PORT STATE SERVICE
21/tcp open ftp
25/tcp open smtp
53/tcp open domain
80/tcp open http
110/tcp open pop3
143/tcp open imap
443/tcp open https
465/tcp open smtps
587/tcp open submission
993/tcp open imaps
995/tcp open pop3s
Nmap done: 1 IP address (1 host up) scanned in 11.62 seconds

3. CONCLUSIONES

Después de realizado este análisis, se encontraron vulnerabilidades como:

- La información como cuentas de correo electrónico de empleados de la entidad, que puede ser usada para él envió de correos fraudulentos, software malicioso o ingeniería social.

- El Crossdomain java script source file inclusion: Esta vulnerabilidad está presente porque no se asegura que la entrada de datos de terceros, este codificada de manera adecuada o porque no se verifica que los datos sean seguros en el momento que ingresan y se incluyen en la página de salida, en el caso de la entidad, los datos considerados como no confiables están basados en el contexto HTML, más puntualmente en Java script.

- Web browser XSS Protection no tenabled: es un error en la configuración ya que no está habilitada la protección contra el Cross Site Scripting.

- X content type options header missing: es un error ya que al no tener habilitada esta cabecera cabe la posibilidad de que se carguen hojas de estilo o scripts maliciosos.

Puertos abiertos vulnerables como:

- 21FTP: tiene muchas vulnerabilidades de seguridad conocidas, un servidor ftp mal configurado puede permitir transferencia de ficheros, troyanos entre otros.

- 25 SMTP: tiene una larga trayectoria de vulnerabilidades, cualquier atacante examinaría detenidamente este puerto.

- 80 HTTP: cada día se descubren nuevos fallos de seguridad en los servidores web, pero al ser usado por la entidad, se recomienda tener mayor atención.

- 110 POP3: puede suponer un riesgo si se usa un servidor pop3 inseguro.

- 143 IMAP: es probablemente uno de los puertos más escaneados, es un sistema relativamente nuevo y dado que sus servidores no han tenido tiempo de maduración, este puerto es susceptible a muchos ataques.

- 443 HTTPS: este puerto no debería estar abierto a menos que realmente se use para comercio seguro vía web.

Anexo J. Declaración de aplicabilidad

Cuadro 22. Declaración de aplicabilidad

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) DECLARACIÓN DE APLICABILIDAD		MINSALUD
VERSIÓN: 1.0	CÓDIGO:	FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

LR: requerimientos legales, CO: obligaciones contractuales, BR/BP: requerimientos del negocio/mejores prácticas adoptadas , RRA: resultado de la valoración de riesgos; TSE: hasta cierto punto

N° del Control	Control	Descripción	Controles seleccionados y razones de selección				Justificación de aplicación o Exclusión	Observaciones
			LR	CO	BR/BP	RRA		
A.5	**Políticas de seguridad de la información**							
A.5.1	**Directrices establecidas por la dirección para la seguridad de la información**							
Objetivo: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.								
A.5.1.1	Políticas para la seguridad de la información	Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.			X		La entidad realizó la modificación de la política de seguridad de la información y se encuentra en aprobación por parte del comité.	
A.5.1.2	Revisión de las políticas para seguridad de la información	Control: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.			X		La entidad realiza revisiones periódicas de la política de seguridad de la información. (Por lo menos una vez al año)	
A.6	**Organización de la seguridad de la información**							
A.6.1	**Organización interna**							
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.								
A.6.1.1	Roles y responsabilidades para la seguridad de información	Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.	x				La entidad tiene establecido los roles y responsabilidades para la seguridad de información	
A.6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	X				La entidad tiene establecido los roles y responsabilidades para la seguridad de información	
A.6.1.3	Contacto con las autoridades	Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes.	x				La entidad mantiene contacto con los entes de control que la vigilan.	
A.6.1.4	Contacto con grupos de interés especial	Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.					La entidad se encuentra registrada y reporta posibles eventos o incidente de seguridad con el Equipo de Respuesta a Incidentes de Seguridad Informática	PONAL / CSIRT
A.6.1.5	Seguridad de la información en la gestión de proyectos	Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.			x		La entidad a través del proceso de Gestión de Tic´s brinda asesoría a los dueños de procesos en terma de seguridad de información se deben tener encuentra para ejecución de un proyecto o plan de adquisición	

Cuadro 22. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) DECLARACIÓN DE APLICABILIDAD							MINSALUD
VERSIÓN: 1.0	CÓDIGO:	FECHA ACTUALIZACIÓN:						PAGINA 1 DE 1
LR: requerimientos legales, CO: obligaciones contractuales, BR/BP: requerimientos del negocio/mejores prácticas adoptadas , RRA: resultado de la valoración de riesgos; TSE: hasta cierto punto								
N° del Control	**Control**	**Descripción**	**Controles seleccionados y razones de selección**				**Justificación de aplicación o Exclusión**	**Observaciones**
			LR	**CO**	**BR/BP**	**RRA**		
A.6.2	**Dispositivos móviles y teletrabajo**							
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.								
A.6.2.1	Política para dispositivos móviles	Control: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.					La entidad en estos momentos no cuenta con una política formar para adoptar medidas de seguridad apropiadas para la seguridad de soporte, para gestionar los riesgos introducidos por el uso dispositivos móviles, pero se encuentra en estudio la posibilidad del desarrollo de la política	
A.6.2.2	Teletrabajo	Control: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.					De acuerdo con lo establecido en la Ley 1221 de 2008 la organización no cuenta con Teletrabajo.	
A.7	**Seguridad de los recursos humanos**							
A.7.1	**Antes de asumir el empleo**							
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.								
A.7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	x				Asistencia Jurídica y Gestión Talento Humano cuentan con un proceso y/ procedimiento de verificación de antecedentes	
A.7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.		x			Se cuenta con la Política de Seguridad de la Información y cláusula de confidencialidad establecida dentro de los contratos	
A.6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	X				La entidad tiene establecido los roles y responsabilidades para la seguridad de información	
A.7.2	**Durante la ejecución del empleo**							
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.								
A.7.2.1	Responsabilidades de la dirección	Control: La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.			x		La política es acatada por medio de una resolución el cual se hace pública y la dirección solicita el cumplimiento por párate de cada uno de los funcionarios y contratistas.	
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo			x		La entidad realiza el desarrollo de actividades las cuales van enfocadas al buen uso de los recursos que se brindan a los funcionarios para el cumplimiento de sus funciones.	

Cuadro 22. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) DECLARACIÓN DE APLICABILIDAD							MINSALUD
VERSIÓN: 1.0	CÓDIGO:	FECHA ACTUALIZACIÓN:						PAGINA 1 DE 1
LR: requerimientos legales, CO: obligaciones contractuales, BR/BP: requerimientos del negocio/mejores prácticas adoptadas , RRA: resultado de la valoración de riesgos; TSE: hasta cierto punto								
N° del Control	**Control**	**Descripción**	**Controles seleccionados y razones de selección**				**Justificación de aplicación o Exclusión**	**Observaciones**
			LR	**CO**	**BR/BP**	**RRA**		
A.7.2.3	Proceso disciplinario	Control: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	x				Para los casos de violaciones de seguridad dependiendo el acceso al cual ingreso sin autorización, se le lleva a cabo un proceso disciplinario.	
7.3	**Terminación o cambio de empleo**							
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.								
A.7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.		x			La entidad por medio del proceso de Gestión de Talento Humano y Asistencia Jurídica tiene definido los motivos por el cual un funcionario se le realiza la terminación del contrato.	
A.8	**Gestión de activos**							
A.8.1	**Responsabilidad por los activos**							
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.								
A.8.1.1	Inventario de activos	Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos	x				La entidad cuenta con un inventario de activos fijos y de información el cual se encuentra a cargo del Grupo de trabajo de Servicios Administrativos y Gestión Tic´s	
A.8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deberían tener un propietario.	x				La entidad cuenta con un inventario de activo de información donde se establecen cada uno de los propietarios de los mismos	
A.8.1.3	Uso aceptable de los activos	Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	x				Se identifica con el uso del manual de seguridad cuales son las reglas que los funcionarios deben de adoptar para el uso de los activos	
A.8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.			x		El proceso de Gestión de Talento Humano realiza junto con el funcionario la entrega de los activos los cuales se encuentran cargados al mismo desde el momento de su vinculación	
A.8.2	**Clasificación de la información**							
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.								
A.8.2.1	Clasificación de la información	Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	x				La entidad tiene en su inventario de activos de información la clasificación de estos y aparte se ha elaborado un procedimiento y una política de Gestión de Activos	

Cuadro 22. (Continuación)

ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) DECLARACIÓN DE APLICABILIDAD							MINSALUD
VERSIÓN: 1.0	CÓDIGO:	FECHA ACTUALIZACIÓN:						PAGINA 1 DE 1
LR: requerimientos legales, CO: obligaciones contractuales, BR/BP: requerimientos del negocio/mejores prácticas adoptadas , RRA: resultado de la valoración de riesgos; TSE: hasta cierto punto								
N° del Control	**Control**	**Descripción**	**Controles seleccionados y razones de selección**				**Justificación de aplicación o Exclusión**	**Observaciones**
			LR	**CO**	**BR/BP**	**RRA**		
A.8.3.1	Gestión de medios removibles	Control: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.					La entidad no cuenta con procedimientos para la gestión de medios removibles	
A.8.3.2	Disposición de los medios	Control: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.					La entidad no realiza destrucción de medios.	
A.8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	x				Se cuenta con un programa de gestión documental, el procedimiento para la actualización y modificación de las tablas de retención documental y demás información a cargo de Gestión Documental.	
A.9	**Control de acceso**							
A.9.1	**Requisitos del negocio para control de acceso**							
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.								
A.9.1.1	Política de control de acceso	Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.			x		Se le otorga claves de acceso a los usuarios con perfiles para la administración de la información, parte se tiene una política de control de acceso, bitácoras de centro de cableado, minutas de vigilancia para entrada y salida de equipos portátiles y bitácora de registro de visitantes	
A.9.1.2	Política sobre el uso de los servicios de red	Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.			x		Al momento de crear un usuario se le asigna un grupo de trabajo específico donde se le brindan los permisos para el ingreso a programas y a unidades de red.	
A.9.2	**Gestión de acceso de usuarios**							
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.								
A.9.2.1	Registro y cancelación del registro de usuarios	Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.			x		Se cuenta con el formato de solicitud de servicios de tecnología.	
A.9.2.2	Suministro de acceso de usuarios	Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.			x		Se cuenta con el formato de solicitud de servicios de tecnología.	
A.9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.			x		Se cuenta con el formato de solicitud de servicios de tecnología.	
A.9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.			x		Se lleva a cabo a través de perfiles en los usuarios para cada uno de los aplicativos.	
A.9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.			x		Con los requerimientos por parte de los procesos se requeriría un control y solicitudes para la revisión de los permisos en los usuarios.	
A.9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.			x		Se cuenta con el formato de solicitud de servicios de tecnología.	**A.9.2.6**

Cuadro 22. (Continuación)

ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) DECLARACIÓN DE APLICABILIDAD		MINSALUD
VERSIÓN: 1.0	CÓDIGO:	FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

LR: requerimientos legales, CO: obligaciones contractuales, BR/BP: requerimientos del negocio/mejores prácticas adoptadas , RRA: resultado de la valoración de riesgos; TSE: hasta cierto punto

N° del Control	Control	Descripción	Controles seleccionados y razones de selección				Justificación de aplicación o Exclusión	Observaciones
			LR	CO	BR/BP	RRA		
A.9.3	**Responsabilidades de los usuarios**							
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.								
A.9.3.1	Uso de la información de autenticación secreta	Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.			x		Se realiza la capacitación específica con la ayuda de la política de seguridad en la información.	
A.9.4	**Control de acceso a sistemas y aplicaciones**							
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.								
A.9.4.1	Restricción de acceso Información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.			x		Se otorgan permisos como restricciones a los sistemas de información para aquellos usuarios que requieren ingresos.	
A.9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.			x		la entidad cuenta con Data Center, el cual reúne las especificaciones técnicas y las condiciones básicas de seguridad las cuales se encuentran en mejora continua	
A.9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.			x		Se tiene establecido dentro de la política de seguridad de la información la gestión de contraseñas	
A.9.4.4	Uso de programas utilitarios privilegiados	Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.			x		Se tiene la herramienta PC SECURE que realiza estas restricciones	
A.9.4.5	Control de acceso a códigos fuente de programas	Control: Se debería restringir el acceso a los códigos fuente de los programas.			x		La entidad no cuenta con la restricción al acceso a los códigos fuentes de los programas	
A.10	**Criptografía**							
10.1	**Controles criptográficos**							
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.								
A.10.1.1	Política sobre el uso de controles criptográficos	Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	x				Se lleva a cabo con la utilización de token para el registro y manejo en la información de alta importancia.	
A.10.1.2	Gestión de llaves	Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.	x				las aplicaciones de con las que cuenta la entidad poseen técnicas criptográficas para las claves de los usuarios en los aplicativos	

Cuadro 22. (Continuación)

ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) DECLARACIÓN DE APLICABILIDAD							MINSALUD
VERSIÓN: 1.0	CÓDIGO:	FECHA ACTUALIZACIÓN:						PAGINA 1 DE 1
LR: requerimientos legales, CO: obligaciones contractuales, BR/BP: requerimientos del negocio/mejores prácticas adoptadas , RRA: resultado de la valoración de riesgos; TSE: hasta cierto punto								
N° del Control	**Control**	**Descripción**	**Controles seleccionados y razones de selección**				**Justificación de aplicación o Exclusión**	**Observaciones**
			LR	**CO**	**BR/BP**	**RRA**		
A.11	**Seguridad física y del entorno**							
A.11.1	**Áreas seguras**							
Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.								
A.11.1.1	Perímetro de seguridad física	Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.					La entidad no cuenta con un sistema de seguridad robusto.	
A.11.1.2	Controles físicos de entrada	Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.			x		Se cuenta con sistemas de vigilancia que controla el acceso a las oficinas e instalaciones	
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.					La entidad no cuenta con un sistema de seguridad robusto.	
A.11.1.4	Protección contra amenazas externas y ambientales	Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.					La entidad no cuenta con un sistema de seguridad robusto.	
A.11.1.5	Trabajo en áreas seguras	Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.			x		Por parte del proceso correspondiente realiza el desarrollo del trabajo con los requerimientos necesarios para evitar riesgos en el daño o accesos no autorizados.	
A.11.1.6	Áreas de despacho y carga	Control: Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.					No aplica para la entidad ya que su función principal no es la operatividad en cuanto a despachos o manejo de carga	
A.11.2	**Equipos**							
Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.								
A.11.2.1	Ubicación y protección de los equipos	Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.					La entidad no cuenta con un sistema de seguridad robusto.	
A.11.2.2	Servicios de suministro	Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.			x		La entidad cuenta con una infraestructura para la protección para el tipo de fallas eléctricas por medio de ups, tomas con corriente regulada y planta eléctrica.	
A.11.2.3	Seguridad del cableado	Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.			x		El cableado en la entidad está protegido ya que cuenta con canaletas desde el Centro de Datos a cada uno de los puntos de red en los procesos.	
A.11.2.4	Mantenimiento de equipos	Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.		x			Se cuenta con contratistas los cuales realizan periódicamente o a solicitud los respectivos mantenimientos tanto a los equipos usuarios como los del Centro de Datos.	
A.11.2.5	Retiro de activos	Control: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa	x				Se cuenta con la minuta de vigilancia para la salida de los equipos. Se cuenta con procedimientos	APGTHGTHPT06 ENTREGA DE CARGOS - APGSAGADPT03 ADMINISTYRACION CUENTAS PERSONALES BIENES DEVOLUTIVOS

Cuadro 22. (Continuación)

ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) DECLARACIÓN DE APLICABILIDAD		PAGINA 1 DE 1
VERSIÓN: 1.0	CÓDIGO:	FECHA ACTUALIZACIÓN:	

LR: requerimientos legales, CO: obligaciones contractuales, BR/BP: requerimientos del negocio/mejores prácticas adoptadas , RRA: resultado de la valoración de riesgos; TSE: hasta cierto punto

N° del Control	Control	Descripción	Controles seleccionados y razones de selección				Justificación de aplicación o Exclusión	Observaciones
			LR	CO	BR/BP	RRA		
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.			x		La entidad por medio de un contratista el cual nos suministra soporte, brinda seguridad para el buen uso de los equipos.	
A.11.2.7	Disposición segura o reutilización de equipos	Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.	x				Desde el proceso Gestión de servicios administrativos se cuenta con un procedimiento Baja de bienes muebles por obsolescencia, inservibles o no necesarios para el funcionamiento de la entidad y formato que tiene el proceso Gestión Tic´s cuando un equipo sale de circulación.	APGSAGADPT24 PROCEDIMIENTO BAJA DE BIENES MUEBLES PÓR OBSOLECENCIA, INSERVIBLES O NO NECESARIOS PARA EL FUNCIONAMIENTO DE LA ENTIDAD - APGTSOPSFO09 FORMATO SALIDA DE CIRCULACION EQUIPO DE COMPUTO
A.11.2.8	Equipos de usuario desatendidos	Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.					La entidad no cuenta con la política	
A.11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.					Se realizan capacitaciones de forma dinámicas para que el usuario adopte de forma cultural el uso de la política.	
A.12	**Seguridad de las operaciones**							
A.12.1	**Procedimientos operacionales y responsabilidades**							
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.								
A.12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.	x				Se cuenta con el Sistema Integral de Gestión de Calidad el cual permite a cada uno de los funcionarios informan sobre los tipos de procedimientos que tienen cada una de los procesos.	
A.12.1.2	Gestión de cambios	Control: Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información	x				Se realiza por medio de un estudio previo el cual pone en contexto lo que se va a realizar para su aprobación.	
A.12.1.3	Gestión de capacidad	Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.					No se tiene política establecida	
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.			x		Se cuenta con áreas independientes por procesos para que no haya accesos no autorizados ni se realicen cambios en los sistemas operaciones de los procesos.	

Cuadro 22. (Continuación)

ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) DECLARACIÓN DE APLICABILIDAD							MINSALUD
VERSIÓN: 1.0	CÓDIGO:	FECHA ACTUALIZACIÓN:						PAGINA 1 DE 1
LR: requerimientos legales, CO: obligaciones contractuales, BR/BP: requerimientos del negocio/mejores prácticas adoptadas , RRA: resultado de la valoración de riesgos; TSE: hasta cierto punto								
N° del Control	**Control**	**Descripción**	**Controles seleccionados y razones de selección**				**Justificación de aplicación o Exclusión**	**Observaciones**
			LR	**CO**	**BR/BP**	**RRA**		
A.12.2	**Protección contra códigos maliciosos**							
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos								
A.12.2.1	Controles contra códigos maliciosos	Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.					Con la adquisición de nuevos programas se ha minimizado el código malicioso y con ello la concientización de los usuarios para el buen uso de las redes y sus accesos.	
A.12.4	**Registro y seguimiento**							
Objetivo: Registrar eventos y generar evidencia.								
A.12.4.1	Registro de eventos	Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	x				Se llevan a cabo planes de auditorías por parte del proceso de seguimiento y evaluación independiente.	
A.12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.	x				Se implementa como procedimiento la protección contra la manipulación de accesos no autorizados.	
A.12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.	x				Se tienen registros sobre el tipo de actividades los cuales realizan tanto usuarios como administradores.	
A.12.4.4	sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.					Dentro de la entidad se encuentran algunos puntos los cuales no están sincronizados con el reloj de servidor para la hora exacta.	
A.12.5	**Control de software operacional**							
Objetivo: Asegurar la integridad de los sistemas operacionales.								
A.12.5.1	Instalación de software en sistemas operativos	Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.					La entidad cuanto con una herramienta de seguridad que permite tener inventariado el Hardware y Software	PCINVENTORY
A.12.6	**Gestión de la vulnerabilidad técnica**							
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.								
A.12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.					Se encuentra en proceso de implementación un sistema de Gestión de Seguridad de la información donde se contemplara el manejo de los incidentes y las vulnerabilidades	
A.12.6.2	Restricciones sobre la instalación de software	Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.			x		la entidad cuenta con la herramienta de seguridad PCSEGURE	

Cuadro 22. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) DECLARACIÓN DE APLICABILIDAD		MINSALUD
VERSIÓN: 1.0	CÓDIGO:	FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

LR: requerimientos legales, CO: obligaciones contractuales, BR/BP: requerimientos del negocio/mejores prácticas adoptadas , RRA: resultado de la valoración de riesgos; TSE: hasta cierto punto

N° del Control	Control	Descripción	Controles seleccionados y razones de selección				Justificación de aplicación o Exclusión	Observaciones
			LR	CO	BR/BP	RRA		
A.12.7	**Consideraciones sobre auditorias de sistemas de información**							
Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.								
A.13.1.1	Controles de redes	Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.			X		Tenemos un sistema de administración de red con el cual se mantiene la seguridad contra amenazas.	
A.13.1.2	Seguridad de los servicios de red	Control: Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.			X		Las características están dadas ya que inicialmente se pactan para la prestación de los servicios de red sean por intermedio de un contratista.	
A.13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.					La entidad cuanta con la segmentación de la red	
A.13.2	**Transferencia de información**							
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.								
A.13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.	X				La entidad cuenta con el procedimiento de transferencia documentales mediante el proceso de Gestión Documental	**APGDOSGEPT05 PROCEDIMIENTO TRANSFERENCIAS DOCUMENTALES AL ARCHIVO CENTRAL**
A.13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.	x				La entidad cuenta con convenios interadministrativo donde se establecen las clausulas sobre intercambio y de medio de protección se debe utilizar para este tránsitos	Convenios interadministrativo COLPENSIONES - MINHACIENDA-MINSALUD
A.13.2.3	Mensajería electrónica	Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.			x		Se cuenta con correo electrónico institucional thunderbird	Correo electrónico institucional
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	x				Desde el proceso de Gestión de Talento Humano y Asistencia Jurídica se expiden la cláusula de confidencialidad. Para los contratistas se refleja en una cláusula del contrato de prestación de servicios.	
A.14	**Adquisición, desarrollo y mantenimientos de sistemas**							
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.								
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.					La entidad se encuentra en proceso de la implementación del sistema de seguridad donde implementara políticas de seguridad	
A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	x				La entidad cuenta con una red de alta velocidad que permite una transferencia eficiente de información entre organismos gubernamentales. Además esta conexión optimiza los servicios que se entregan a los ciudadanos.	GNAP
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada					La entidad cuenta con una red de alta velocidad que permite una transferencia eficiente de información entre organismos gubernamentales. Además esta conexión optimiza los servicios que se entregan a los ciudadanos.	GNAP

Cuadro 22. (Continuación)

ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) DECLARACIÓN DE APLICABILIDAD							MINSALUD
VERSIÓN: 1.0	CÓDIGO:	FECHA ACTUALIZACIÓN:						PAGINA 1 DE 1
LR: requerimientos legales, CO: obligaciones contractuales, BR/BP: requerimientos del negocio/mejores prácticas adoptadas , RRA: resultado de la valoración de riesgos; TSE: hasta cierto punto								
N° del Control	**Control**	**Descripción**	**Controles seleccionados y razones de selección**				**Justificación de aplicación o Exclusión**	**Observaciones**
			LR	**CO**	**BR/BP**	**RRA**		
A.14.2	**Seguridad en los procesos de desarrollo y soporte**							
Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.								
A.14.2.1	Política de desarrollo seguro	Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.					No se tiene política establecida	
A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.			x		Se tiene un procedimiento y un formato en donde se registra los cambios de hardware, así mismo se informa a el Proceso Gestión de servicios administrativos	
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.			x		Se cuenta con un Procedimiento donde incluye revisiones técnicas de las aplicaciones.	
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.			x		la entidad cuenta con una política y un aplicativo de seguridad que restringe la instalación de software no autorizado	
A.14.2.5	Principios de construcción de sistemas seguros	Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.					No se tiene política establecida	
A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.					No se tiene política establecida	
A.14.2.7	Desarrollo contratado externamente	Control: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	x				En el proceso de Asistencia Jurídica se asigna un interventor del contrato y este es el encargado de supervisar y monitorear la ejecución del contrato.	
A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.					Se realiza el Procedimiento hace pruebas de funcionalidad pero no está documentado	
A.14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.					Se realiza el Procedimiento hace pruebas de funcionalidad pero no está documentado	
14.3	**Datos de prueba**							
Objetivo: Asegurar la protección de los datos usados para pruebas.								
A.14.3.1	Protección de datos de prueba	Control: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.					No se tiene política establecida	

Cuadro 22. (Continuación)

ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) DECLARACIÓN DE APLICABILIDAD		PAGINA 1 DE 1
VERSIÓN: 1.0	CÓDIGO:	FECHA ACTUALIZACIÓN:	

LR: requerimientos legales, CO: obligaciones contractuales, BR/BP: requerimientos del negocio/mejores prácticas adoptadas , RRA: resultado de la valoración de riesgos; TSE: hasta cierto punto

N° del Control	Control	Descripción	Controles seleccionados y razones de selección				Justificación de aplicación o Exclusión	Observaciones
			LR	CO	BR/BP	RRA		
A.15	**Relación con los proveedores**							
A.15.1	**Seguridad de la información en las relaciones con los proveedores**							
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.								
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar.			X		Política de seguridad de la información	
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.			X		Política de seguridad de la información y contratos	
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.			X		Política de seguridad de la información y contratos	
A.15.2	**Gestión de la prestación de servicios con los proveedores**							
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.								
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	x				Se realiza seguimientos a los servicios prestados a la entidad por terceros ya que con ello se evalúa con la terminación del contrato para siguientes solicitudes.	
A.15.2.2	Gestión de cambios en los servicios de proveedores	Control: Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos	x				Se realiza seguimientos a los servicios prestados a la entidad por terceros ya que con ello se evalúa con la terminación del contrato para siguientes solicitudes.	
A.16	**Gestión de incidentes de seguridad de la información**							
A.16.1	**Gestión de incidentes y mejoras en la seguridad de la información**							
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades								
A.16.1.1	Responsabilidad y procedimientos	Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.					Se encuentra en proceso de implementación un sistema de Gestión de Seguridad de la información donde se contemplara el manejo de los incidentes y las vulnerabilidades	
A.16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.					Se encuentra en proceso de implementación un sistema de Gestión de Seguridad de la información donde se contemplara el manejo de los incidentes y las vulnerabilidades	
A.16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.					Se encuentra en proceso de implementación un sistema de Gestión de Seguridad de la información donde se contemplara el manejo de los incidentes y las vulnerabilidades	

Cuadro 22. (Continuación)

FONDO DE PASIVO SOCIAL FERROCARRILES NACIONALES DE COLOMBIA ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) DECLARACIÓN DE APLICABILIDAD		MINSALUD
VERSIÓN: 1.0	CÓDIGO:	FECHA ACTUALIZACIÓN:	PAGINA 1 DE 1

LR: requerimientos legales, CO: obligaciones contractuales, BR/BP: requerimientos del negocio/mejores prácticas adoptadas , RRA: resultado de la valoración de riesgos; TSE: hasta cierto punto

N° del Control	Control	Descripción	Controles seleccionados y razones de selección				Justificación de aplicación o Exclusión	Observaciones
			LR	CO	BR/BP	RRA		
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.					Se encuentra en proceso de implementación un sistema de Gestión de Seguridad de la información donde se contemplara el manejo de los incidentes y las vulnerabilidades	
A.16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.					Se encuentra en proceso de implementación un sistema de Gestión de Seguridad de la información donde se contemplara el manejo de los incidentes y las vulnerabilidades	
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.					Se encuentra en proceso de implementación un sistema de Gestión de Seguridad de la información donde se contemplara el manejo de los incidentes y las vulnerabilidades	
A.16.1.7	Recolección de evidencia	Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.					Se encuentra en proceso de implementación un sistema de Gestión de Seguridad de la información donde se contemplara el manejo de los incidentes y las vulnerabilidades	
A.17	**Aspectos de seguridad de la información de la gestión de continuidad de negocio**							
A.17.1	**Continuidad de seguridad de la información**							
Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización								
A.17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.			x		la entidad cuenta con un plan de contingencia pero se encuentra desactualizada y ha definido una política de continuidad de negocio	
A.17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.			x		la entidad cuenta con un plan de contingencia pero se encuentra desactualizo y ha definido una política de continuidad de negocio	
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.			x		La entidad no ha realizado verificación, revisión y evaluación de la continuidad de la seguridad de la información	
A.17.2	**Redundancias**							
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.								
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.					La entidad no cuenta este control	

Cuadro 22. (Continuación)

ADMINISTRACIÓN DEL SISTEMA INTEGRAL DE GESTIÓN (MECI-CALIDAD)	SISTEMA INTEGRAL DE GESTIÓN (MECI – CALIDAD) DECLARACIÓN DE APLICABILIDAD		PAGINA 1 DE 1
VERSIÓN: 1.0	CÓDIGO:	FECHA ACTUALIZACIÓN:	

LR: requerimientos legales, CO: obligaciones contractuales, BR/BP: requerimientos del negocio/mejores prácticas adoptadas , RRA: resultado de la valoración de riesgos; TSE: hasta cierto punto

N° del Control	Control	Descripción	Controles seleccionados y razones de selección				Justificación de aplicación o Exclusión	Observaciones
			LR	CO	BR/BP	RRA		
A.18	**Cumplimiento**							
A.18.1	**Cumplimiento de requisitos legales y contractuales**							
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.								
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	x				La entidad lleva a cabo la implementación de leyes aplicables por medio del Normograma Institucional.	
A.18.1.2	Derechos de propiedad intelectual	Control: Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	x				Se cuenta con el servicio de licenciamiento de software.	
A.18.1.3	Protección de registros	Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	x				La entidad protege cada uno de sus registros por medio del programa de correspondencia Orfeo el cual nos brinda la garantía en la operación.	
A.18.1.4	Privacidad y protección de datos personales	Control: Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.	x				Se adopta la ley de protección de datos. Se cuenta con política de protección de datos personales.	
A.18.1.5	Reglamentación de controles criptográficos	Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	x				la entidad cuenta con medios digitales avalados por una entidad certificadora	
A.18.2	**Revisiones de seguridad de la información**							
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.								
A.18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.					La entidad esta fase de implementación del sistema de gestión de seguridad de la información y tiene previsto la revisión periódica del mismo	
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.			x		Se cumple con los requerimientos hechos por la directiva por medio de la política de seguridad.	
A.18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.			x		En la entidad el proceso de Tic's realiza seguimiento y control para cumplir con los lineamientos en cuanto a seguridad e integridad de la información.	

FUENTE: Autores - Declaración de aplicabilidad