MINSALUD

FONDO DE PASIVO SOCIAL
FERROCARRILES NACIONALES DE COLOMBIA

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

RESOLUCIÓN NUMERO 0846 **DE** 09 JUN 2017

POR MEDIO DE LA CUAL SE DETERMINA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SE DEROGA LA RESOLUCION 2130 DE 2014 Y ESTABLECEN OTRAS DISPOSICIONES.

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:

Que la constitución política de Colombia en su artículo 15, consagra que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, debiendo el estado respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.

Que la constitución política de Colombia en su artículo 209, establece que La función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones. Las autoridades administrativas deben coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado. La administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley.

Que el decreto 1078 de 2015 dispone que las entidades que conforma la administración pública serán sujetos obligados para el cumplimiento de las políticas y los lineamientos de la estrategia de gobierno en línea, estableciendo en su artículo 2.2.9.1.2.1 como uno de sus cuatro componentes el de la seguridad y privacidad de la información, comprendido por las acciones trasversales a los componentes de TIC para servicios, TIC para Gobierno Abierto y TIC para la Gestión, tendientes a proteger la información y sistemas de información, el acceso, divulgación, interrupción o destrucción no autorizada.

Que mediante la resolución N° 2130 del 27 de agosto 2014, el Fondo adoptó la política de seguridad de la información.

RESOLUCIÓN NUMERO 0846 **DE** 09 JUN 2017

POR MEDIO DE LA CUAL SE DETERMINA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SE DEROGA LA RESOLUCION 2130 DE 2014 Y ESTABLECEN OTRAS DISPOSICIONES.

Política de Seguridad y Privacidad de la Información

El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.
Para el Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia (FPS- FNC), la seguridad y privacidad de la información busca 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.
Que, en mérito de lo expuesto,

RESUELVE:

CAPITULO I DISPOSICIONES GENERALES

ARTÍCULO PRIMERO. Objeto. La presente resolución tiene como objeto la actualización de la política de seguridad de la información del Fondo Pasivo Social Ferrocarriles Nacionales de Colombia, así como definir lineamientos frente a su uso y manejo.

ARTÍCULO SEGUNDO: Objetivos de la Política de Seguridad y privacidad de la Información

Objetivo General

Determinar los lineamientos que permitan proteger los activos de información del Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia mediante mecanismos de aseguramiento que permitan el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y no repudio de la información del FPS- FNC.

Objetivos Especificos

- 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.

RESOLUCIÓN NUMERO 0846 **DE** 09 JUN 2017

POR MEDIO DE LA CUAL SE DETERMINA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SE DEROGA LA RESOLUCION 2130 DE 2014 Y ESTABLECEN OTRAS DISPOSICIONES.

- 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, física 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 servidores públicos, contratistas, terceros, proveedores del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA (FPS -FNC) y la ciudadanía en general.

ARTÍCULO CUARTO: Roles y Responsabilidades

Encargado de la seguridad de la información: Serán funciones del 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 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 pruebas que hayan sido utilizada.
- Mantener un inventario de los activos de información en la entidad y clasificarlos según sea su tipo con la participación activa de los procesos de la Entidad.

RESOLUCIÓN NUMERO 0846 DE 09 JUN 2017

POR MEDIO DE LA CUAL SE DETERMINA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SE DEROGA LA RESOLUCION 2130 DE 2014 Y ESTABLECEN OTRAS DISPOSICIONES.

- 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 a través del programa anual de auditoria establecido por la entidad.
- Asesorar a la entidad en temas seguridad de la información.
- 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 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:

- Cumplir con la política de seguridad y privacidad de la información aprobada por el comité de desarrollo administrativo.

0846

RESOLUCIÓN NUMERO **DE** 09 JUN 2017

POR MEDIO DE LA CUAL SE DETERMINA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SE DEROGA LA RESOLUCION 2130 DE 2014 Y ESTABLECEN OTRAS DISPOSICIONES.

- Asignar los niveles iníciales de clasificación de información.
- Revisión y actualización por lo menos una vez al año 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, con la asesoría del encargado de seguridad de la información.

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 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 FPS -FNC 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 y/o reportar los incidentes de seguridad, mal uso de los recursos y eventos sospechosos de los que tenga conocimiento.
- 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.

RESOLUCIÓN NUMERO 0846 DE 09 JUN 2017

POR MEDIO DE LA CUAL SE DETERMINA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SE DEROGA LA RESOLUCION 2130 DE 2014 Y ESTABLECEN OTRAS DISPOSICIONES.

- Garantizar la protección de la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
- Acatar y dar cumplimiento a los lineamientos dispuestos la política de seguridad y privacidad de la información.

CAPITULO II POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO QUINTO: Política del Sistema de Gestión de Seguridad de la Información

El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia (FPS -FNC) encargada de proteger las prestaciones económicas legales y convencionales a los extrabajadores, pensionados y beneficiarios de las liquidadas empresas Ferrocarriles Nacionales de Colombia y ALCALIS y de administrar los servicios de salud a los pensionados y beneficiarios de la empresa liquidada Ferrocarriles Nacionales y Puertos de Colombia; de acuerdo a los lineamientos establecidos en la norma ISO 27001:2013 y en concordancia con la normatividad vigente aplicada como lo es MECI (Modelo Estándar de Control Interno), Gobierno en línea, demás normatividad aplicables y vigentes al sistema de Gestión de Seguridad de la Información se compromete a:

- Definir, Implementar, Operar y Mejorar 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.
- Definir las responsabilidades frente a la seguridad de la información compartida, publicada y aceptadas por cada uno de los funcionarios, proveedores o terceros.
- Proteger 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.
- Definir y Establecer 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.
- Proteger su información de las amenazas originadas por parte del personal.
- Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

RESOLUCIÓN NUMERO 0846 **DE** 09 JUN 2017

POR MEDIO DE LA CUAL SE DETERMINA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SE DEROGA LA RESOLUCION 2130 DE 2014 Y ESTABLECEN OTRAS DISPOSICIONES.

- Controlar la operación de sus procesos garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Implementar control de acceso a la información, sistemas y recursos de red.
- Garantizar que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- Garantizar 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.
- Garantizar la disponibilidad de sus procesos y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- Garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.
- Garantizar el uso de software autorizado y/o adquirido legalmente por la entidad.
- Cualquier auditoria de seguridad a los sistemas del FPS - FNC debe estar debidamente autorizada y aprobada por el jefe de oficina asesora de Planeación y sistemas, con visto bueno del Director.
- Proveer el personal para realizar las auditorías internas de seguridad y privacidad de la información.
- Cumplir con la política de buen uso y manejo de los equipos de cómputo, los servicios institucionales de correo electrónico e internet.

Para alcanzar esta política debe existir el compromiso de alta dirección y todos los responsables de los procesos de la entidad, fortaleciendo de la cultura y las competencias del personal en tema de seguridad y privacidad de la información y destinando recursos.

CAPITULO III LINEAMIENTOS POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ARTÍCULO SEXTO: Lineamiento 1 Estructura organizacional de seguridad de la información

El FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA

RESOLUCIÓN NUMERO 0846 **DE** 09 JUN 2017

POR MEDIO DE LA CUAL SE DETERMINA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SE DEROGA LA RESOLUCION 2130 DE 2014 Y ESTABLECEN OTRAS DISPOSICIONES.

(FPS – FNC) 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 (FPS – FNC):

- La Alta Dirección del FONDO DE PASIVO SOCIAL DE FERROCARRILES NACIONALES DE COLOMBIA (FPS – FNC) 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, 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.

RESOLUCIÓN NUMERO 0346 DE 09 JUN 2017

POR MEDIO DE LA CUAL SE DETERMINA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SE DEROGA LA RESOLUCION 2130 DE 2014 Y ESTABLECEN OTRAS DISPOSICIONES.

- La Oficina de Control Interno, 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 debe informar a las personas y áreas responsables cuando se encuentren hallazgos durante las auditorias.
- La Alta Dirección 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 SEPTIMO: lineamiento 2 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.

RESOLUCIÓN NUMERO 0846 **DE** 09 JUN 2017

POR MEDIO DE LA CUAL SE DETERMINA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SE DEROGA LA RESOLUCION 2130 DE 2014 Y ESTABLECEN OTRAS DISPOSICIONES.

- 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 OCTAVO: lineamiento 3 Seguridad de los Recursos Humanos

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 deberá incluir en la minutas de los contratista cualquiera que sea su modalidad, las clausula u obligaciones correspondiente a la seguridad de la información con el fin de reducir el riesgo de robo, fraude, mal uso de las instalaciones y medios, asegurando la confidencialidad, disponibilidad e integridad de la información.
- Cada Supervisor de Contrato, jefe inmediato y/o similar debe constatar la existencia de Acuerdos y/o Cláusulas correspondiente a la seguridad de la información 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 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 NOVENO: Lineamiento 4 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

RESOLUCIÓN NUMERO 0846 DE 09 JUN 2017

POR MEDIO DE LA CUAL SE DETERMINA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SE DEROGA LA RESOLUCION 2130 DE 2014 Y ESTABLECEN OTRAS DISPOSICIONES.

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.
- 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 como cada tres mes y por seguridad deben ser alfanumérica de mínimo 8 caracteres e que deben cumplir con las siguientes características: Incluir combinación de números, letras mayúsculas, letras minúsculas y caracteres especiales; No se permite el préstamo de claves y contraseñas.

ARTÍCULO DECIMO: Lineamiento 5 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.

RESOLUCIÓN NUMERO 0846 DE 09 JUN 2017

POR MEDIO DE LA CUAL SE DETERMINA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SE DEROGA LA RESOLUCION 2130 DE 2014 Y ESTABLECEN OTRAS DISPOSICIONES.

- Los funcionarios y/o contratistas 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 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), mensajeria 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 encargado de la 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 PRIMERO: lineamento 6 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.

RESOLUCIÓN NUMERO 0846 DE 09 JUN 2017

POR MEDIO DE LA CUAL SE DETERMINA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SE DEROGA LA RESOLUCION 2130 DE 2014 Y ESTABLECEN OTRAS DISPOSICIONES.

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.
- Los visitantes deben ser acompañados por el funcionario o contratista del Fondo que avala el ingreso, durante el tiempo que dure la visita.

ARTÍCULO DECIMO SEGUNDO: lineamiento 7 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 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.

RESOLUCIÓN NUMERO 0846 **DE** 09 JUN 2017

POR MEDIO DE LA CUAL SE DETERMINA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SE DEROGA LA RESOLUCION 2130 DE 2014 Y ESTABLECEN OTRAS DISPOSICIONES.

- 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 reglamentada por Capítulo 2 del Título 1 de la Parte 1 del decreto 1081 de 2015, la ley 594 de 2000 (ley general de archivo), decreto 1080 de 2015 y la ley 1581 de 2012
- 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.
- El proceso de gestión documental con el acompañamiento del oficial de seguridad deben implementar los controles necesarios para que los archivos de gestión cuenten con los mecanismos de seguridad de la información para el mitigar de vulnerar la confidencialidad, integridad y disponibilidad de la información.

ARTÍCULO DECIMO TERCERO: lineamiento 8 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.

RESOLUCIÓN NUMERO 0846 DE 09 JUN 2017

POR MEDIO DE LA CUAL SE DETERMINA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SE DEROGA LA RESOLUCION 2130 DE 2014 Y ESTABLECEN OTRAS DISPOSICIONES.

- 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 DECIMO CUARTO: lineamiento 9 protecciones 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 DECIMO QUINTO: lineamiento 10 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

RESOLUCIÓN NUMERO 0846 DE 09 JUN 2017

POR MEDIO DE LA CUAL SE DETERMINA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SE DEROGA LA RESOLUCION 2130 DE 2014 Y ESTABLECEN OTRAS DISPOSICIONES.

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 para los lineamientos de 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 que manejan las plataformas tecnológicas de la entidad, el identificar la información considerada como critica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

ARTÍCULO DECIMO SEXTO: lineamiento 11 gestiones 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 DECIMO SEPTIMO: lineamiento 12 tratamientos de datos personales

En cumplimiento de la de Ley 1581 de 2012 y su decreto reglamentario, por la cual se dictan disposiciones para la protección de datos personales, el FONDO DE PASIVO SOCIAL DE

RESOLUCIÓN NUMERO 0846 DE 09 JUN 2017

POR MEDIO DE LA CUAL SE DETERMINA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SE DEROGA LA RESOLUCION 2130 DE 2014 Y ESTABLECEN OTRAS DISPOSICIONES.

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 de los datos personales

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:

1. Garantizar al Titular de los datos personales, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;

2. Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular de los datos personales;

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

RESOLUCIÓN NUMERO 0846 **DE** 09 JUN 2017

POR MEDIO DE LA CUAL SE DETERMINA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SE DEROGA LA RESOLUCION 2130 DE 2014 Y ESTABLECEN OTRAS DISPOSICIONES.

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

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

6. 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;

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

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

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

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

11. 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;

12. 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;

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

14. 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.

15. 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 (FPS - FNC):

- El FPS - FNC 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 de los datos personales. Sin embargo, cuando no corresponda a sus funciones deberá obtener la

RESOLUCIÓN NUMERO 0846 DE 09 JUN 2017

POR MEDIO DE LA CUAL SE DETERMINA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SE DEROGA LA RESOLUCION 2130 DE 2014 Y ESTABLECEN OTRAS DISPOSICIONES.

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 FPS - FNC 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 y decreto 1759 de 2016.

- 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 calle 13 No. 18 – 24 en el proceso de Atenciónal 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 FPS - FNC implementara procedimiento para garantizar el cumplimiento de la política de tratamiento de datos personales.

RESOLUCIÓN NUMERO 0846 **DE** 09 JUN 2017

POR MEDIO DE LA CUAL SE DETERMINA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SE DEROGA LA RESOLUCION 2130 DE 2014 Y ESTABLECEN OTRAS DISPOSICIONES.

CAPITULO IV DIFUSIÓN, REVISION, NIVEL DE CUMPLIMIENTO, INCUMPLIMIENTO Y VIGENCIA

ARTÍCULO DECIMO OCTAVO: Difusión. El Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia (FPS - FNC) 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 FPS - FNC a través del link respectivamente y se le informará a cada funcionario a través de correo masivo u otras actividades de difusión que se definan para tal efecto
Será responsabilidad del proceso de Gestión de Talento humano 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.
Será responsabilidad de la oficina asesora jurídica incorporar dentro de los contratos cláusula de cumplimiento de las Políticas de Seguridad y Privacidad de la Información, cual deben ser entregadas para su consentimiento y firma de las mismas.
El jefe de la oficina asesora de planeación y sistemas será el responsable de la existencia permanente y el cumplimiento de un plan formal de difusión, capacitación y sensibilización de la seguridad de la información.
El Encargado de Seguridad de la información es el responsable de la ejecución del plan y el cumplimiento de sus objetivos, así como la existencia de un plan comunicacional que lo complemente.

ARTÍCULO NOVENO: 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 VIGÉSIMO: 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

RESOLUCIÓN NUMERO 0846 **DE** 09 JUN 2017

POR MEDIO DE LA CUAL SE DETERMINA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SE DEROGA LA RESOLUCION 2130 DE 2014 Y ESTABLECEN OTRAS DISPOSICIONES.

- 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 VIGÉSIMO PRIMERO: 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.

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

ARTÍCULO VIGÉSIMO TERCERO: Vigencias. La presente resolución rige a partir de la fecha de su expedición.

ARTÍCULO VIGÉSIMO CUARTO: Derogatorias. La presente resolución deroga la resolución 2130 de 2014 y todas las demás resoluciones que sean contrarias.

COMUNICASE Y CUMPLASE:

JOSÉ JAIME AZAR MOLINA
Director General (E)

Proyectó: Roselys Silva Cuadrado
Revisó: Rita Omaira Martínez Avellaneda
Jefe de la Oficina Asesora de Planeación y Sistemas (E)

Dema Consuelo Fernández Rodriguez
Profesional VIII