POLÍTICA DE GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN

EMPRESA FÉRREA REGIONAL S.A.S

BOGOTÁ, DICIEMBRE 2021

Calle 26 No. 69 - 76 – oficinas 1103 y 1104
Torre 1, Edificio Elemento Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (571) 7458897
www.efr-cundinamarca.gov.co
@efrcundinamarca @efrcundinamarca @efrcundinamarca

CONTROL DE CAMBIOS		
1	03/11/2020	Creación del documento.
2	2/12/2021	Inclusión de políticas Inclusión de Normatividad

RESPONSABLES	CARGO	NOMBRE	FIRMA
APROBÓ	Subgerente General	Oscar Eduardo Rodríguez Lozano	
REVISÓ	Directora Administrativa y Financiera	Fanny Rodríguez Torres	
	Jefe Oficina Asesora de Planeación Institucional	Esteban Mancera Orjuela	
ELABORÓ	Contratista Oficina Asesora de Planeación	Katherine Rodríguez	
	Contratista Dirección Administrativa y Financiera	Berny Duitama	

Calle 26 No. 69 - 76 – oficinas 1103 y 1104
Torre 1, Edificio Elemento Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (571) 7458897
www.efr-cundinamarca.gov.co
@efrcundinamarca @efrcundinamarca @efrcundinamarca

CONTENIDO

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN 4
1. INTRODUCCIÓN 4
2. OBJETIVO 6
3. ALCANCE 6
4. MARCO NORMATIVO 6
5. DEFINICIONES 8
6. COMPROMISO DE LA ALTA DIRECCIÓN 10
7. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN 11
8. APLICABILIDAD 28

Calle 26 No. 69 - 76 – oficinas 1103 y 1104
Torre 1, Edificio Elemento Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (571) 7458897
www.efr-cundinamarca.gov.co
@efrcundinamarca @efrcundinamarca @efrcundinamarca

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de Empresa Férrea Regional SAS, con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

Empresa Férrea Regional, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- ✓ Minimizar el riesgo de los procesos misionales de la entidad.
- ✓ Cumplir con los principios de seguridad de la información.
- ✓ Cumplir con los principios de la función administrativa.
- ✓ Mantener la confianza de los funcionarios, contratistas y terceros.
- ✓ Apoyar la innovación tecnológica.
- ✓ Implementar el sistema de gestión de seguridad de la información.
- ✓ Proteger los activos de información.
- ✓ 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, aprendices, practicantes y clientes del Empresa Férrea Regional SAS.
- ✓ Garantizar la continuidad del negocio frente a incidentes.

1. INTRODUCCIÓN

En esta versión de la política, se incluyen nuevos lineamientos que permitan administrar la seguridad de la información dentro de la Empresa Férrea Regional S.A.S., así como establecer un marco gerencial para iniciar y controlar su implementación, para que con ello se pueda aplicar medidas de seguridad adecuadas en los accesos a funcionarios, trabajadores oficiales y contratistas de prestación de servicios a la información de la EFR S.A.S.

La información junto a los procesos y sistemas que hacen uso de ella, son activos significativos de una organización. La confidencialidad, integridad y disponibilidad de información sensible logran llegar a ser esenciales para amparar los niveles de competitividad, rentabilidad, conformidad legal e imagen precisos para lograr los objetivos de la entidad y afirmar el cumplimiento de objetivos misionales.

Las organizaciones y sus sistemas de información son sensibles a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "hacking" o los ataques de denegación de servicio son unos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad producidos voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallas técnicas.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento dentro de una organización. Es así como, estos tres términos constituyen la base sobre la que se funda todo el edificio de la seguridad de la información:

- ✓ Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- ✓ Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- ✓ Disponibilidad: acceso y uso de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

De esta forma, y teniendo en cuenta la importancia de los proyectos que lidera la Empresa Férrea Regional SAS-EFR, es fundamental definir las necesidades de sus grupos de interés y la valoración de los controles precisos para mantener la seguridad de la información, para lo cual, se debe establecer una política que tenga en cuenta el marco general del funcionamiento de la Entidad, sus objetivos institucionales, sus procesos misionales y que este adaptada a las condiciones específicas y particulares de cada área de la Empresa según corresponda, y para que sea implementada y resguardada por la Dirección Administrativa y Financiera y acogida por todos los funcionarios y contratistas de la Empresa.

De esta forma, la EFR define una política para la gestión y seguridad de su información, la cual tendrá los criterios de ser sucinta, fácil de leer y comprender, flexible y fácil de hacer cumplir para todos aquellos dentro del alcance sin excepción. Está Políticas le permite a la Empresa tomar decisiones más ágiles y acertadas frente a los riesgos y las regulaciones, permitiendo una gestión oportuna y efectiva aprovechando de la mejor forma los activos con que cuenta,

2. OBJETIVO

Establecer los lineamientos para proteger, preservar y administrar correctamente la información de la Empresa Férrea Regional SAS., junto con las tecnologías utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el desempeño de las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no rechazo de la información.

3. ALCANCE

Esta política aplica a todas las áreas que componen la Empresa Férrea Regional SAS, a todos los activos de información, a la totalidad de los procesos internos o externos vinculados a la misma a través de contratos o acuerdos con terceros y a todo el personal que labora en ella cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe que tengan acceso a los servicios de red, aplicaciones y sistemas de información y a las grupos de interés que accedan o hagan uso de cualquier activo de información independientemente de su ubicación, medio o formato.

4. MARCO NORMATIVO

- ✓ Constitución Política de Colombia. Artículo 15.
- ✓ Ley 44 de 1993 "por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944." (Derechos de autor).
- ✓ Ley 527 de 1999 "por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".
- ✓ Ley 594 de 2000 "Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones". ✓ Ley 734 de 2002 "Por la cual se expide el Código Disciplinario Único".
- ✓ Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- ✓ Ley 1221 del 2008. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- ✓ Ley 1273 de 2009 "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones
- ✓ CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.

- ✓ Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- ✓ Decreto 0884 del 2012. Por el cual se reglamenta parcialmente la Ley 1221 del 2008.
- ✓ Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales".
- ✓ Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- ✓ Ley 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".
- ✓ Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- ✓ Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- ✓ Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- ✓ CONPES 3854 de 2016 – Política de Seguridad Digital del Estado Colombiano
- ✓ Decreto 1499 de 2017, el cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión.
- ✓ Decreto 1083 de 2015 sustituido por el artículo 1º del Decreto 1499 de 2017 - políticas de Gestión y Desempeño Institucional, ("11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital)
- ✓ Decreto 728 de 2017. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
- ✓ Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

5. DEFINICIONES

Para efectos de la aplicación de las políticas se adoptan las siguientes definiciones:

- ✓ **ACTIVOS DE INFORMACIÓN:** Cualquier componente (humano, tecnológico, software, manuales, documentación, entre otros) que tiene valor para la organización y signifique riesgo si llega a manos de personas no autorizadas.

- ✓ **ACTIVOS DE INFORMACIÓN CRÍTICOS:** Activo de información cuya afectación o alteración puede generar un impacto negativo de carácter económico, legal o al buen nombre de la institución.

- ✓ **ARCHIVO:** Colección de datos e información del mismo tipo, almacenada en forma organizada como una unidad, que puede emplearse y tratarse como soporte material de la información contenida en éstos.

- ✓ **APLICACIÓN:** Programa informático diseñado para permitir a los usuarios la realización de tareas específicas en computadores, servidores y similares.

- ✓ **BASE DE DATOS:** Conjunto de datos almacenados y organizados con el fin de facilitar su acceso y recuperación.

- ✓ **BACKUPS O COPIAS DE RESPALDO:** Copia que se realiza a la información institucional definida como sensible o vulnerable, con el fin de utilizarla posteriormente para restablecer el original ante una eventual pérdida de datos, para continuar con las actividades rutinarias y evitar pérdida generalizada de datos.

- ✓ **CATEGORÍAS DE INFORMACIÓN:** Toda información de contenido o estructura homogénea, sea física o electrónica, emanada de un mismo sujeto obligado como resultado del ejercicio de sus funciones y que pueda agruparse a partir de categorías, tipos o clases según sus características internas (contenido) o externas (formato o estructura). Decreto 103/2015

- ✓ **CIO:** Chief Information Officer

- ✓ **CLASIFICAR:** Acto de asignar a la información alguna de las categorías definidas por la Entidad: Reservada, clasificada, Documento en construcción, Pública.

- ✓ **CONFIDENCIALIDAD:** Propiedad de la información que determina que esté disponible a personas autorizadas.

- ✓ **CÓDIGO FUENTE:** Conjunto de instrucciones escritas en algún lenguaje de programación de computadoras, hechas para ser leídas y transformadas por alguna

herramienta de software (compilador, intérprete, ensamblador) en lenguaje de máquina o instrucciones ejecutables en el computador.

- ✓ **CREDENCIALES DE ACCESO:** Privilegios de seguridad agrupados bajo un nombre y contraseña, que permiten acceso a los sistemas de información.

- ✓ **CRIPTOGRAFÍA:** Es una de las disciplinas más relevantes dentro del campo de la seguridad de la información. A la hora de proteger los datos y la información que manejan las organizaciones, tanto física como digital, las técnicas criptográficas están ganando mucho peso en la actualidad. Por ello, todo profesional que aspire a ocupar puestos especializados en **Ciberseguridad y Riesgos Digitales**, debe saber **qué es la criptografía** y cuáles son sus principales aplicaciones.

- ✓ **CUSTODIO:** Es el encargado de gestionar y administrar la adecuada operación del activo y la información relacionada con éste. En ocasiones el responsable y el custodio son la misma persona.

- ✓ **DATACENTER, CENTRO DE DATOS O SALA DE SERVIDORES:** Área dispuesta para el alojamiento seguro de los equipos de cómputo necesarios para el procesamiento y almacenamiento de la información de una organización (Servidores, SAN, equipos de comunicación, etc.).

- ✓ **DISPOSITIVO BIOMÉTRICO:** Dispositivo de seguridad utilizado en sistemas computarizados que sirve para identificar atributos físicos como rasgos faciales, patrones oculares, huellas digitales, la voz y la escritura.

- ✓ **DISPOSITIVO MÓVIL:** Aparato electrónico con capacidades de cómputo y conexión a redes inalámbricas cuyo tamaño y diseño permite ser fácilmente transportado para utilizarse en diversas ubicaciones con facilidad (portátiles, tablets, celulares inteligentes y demás dispositivos con características similares).

- ✓ **INFORMACIÓN:** Todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

- ✓ **INFORMACIÓN SENSIBLE O VULNERABLE:** También llamado activo sensible, es el nombre que recibe la información personal o institucional (datos personales, información financiera, contraseñas de correo electrónico, datos personales, datos de investigaciones), la cual puede ser alterada, descompuesta, mal utilizada, divulgada y/o eliminada, causando graves daños a la organización propietaria.

- ✓ **NIVELES DE BACKUP:** Se refiere a la cantidad de copias o respaldos que se tiene de datos determinados. Si se cuenta con una sola copia, se está hablando de un backup de

1er. Nivel; si se tienen dos copias, de un backup de 2do. Nivel. Cuanto mayor sea el número de niveles de backup, menor será el riesgo de perder los datos.

- ✓ **PROPIETARIO:** En la estructura administrativa de la institución, se le otorga la propiedad del activo a cada una de las unidades estratégicas, divisiones organizacionales, gerencias, rectorías o vicerrectorías.

- ✓ **REPORTES BÁSICOS ACADÉMICOS (RBA):** Son aquellos informes generados por el sistema de información institucional que soportan o sirven de base para la toma de decisiones en la gestión académica y el reporte a los organismos de inspección, control y vigilancia, tanto en el ámbito interno como externo.

- ✓ **RESPONSABLE**: El jefe de área o gerente de cada una de dichas áreas, será el responsable ante la Institución, de los activos de información registrados como de su propiedad.

- ✓ **SAN** (Storage Área Network) O Red de Área de Almacenamiento: recurso compartido, empleado como repositorio de información institucional tanto de funcionarios, docentes y/o contratistas como de grupos y unidades funcionales, donde se definen permisos de acceso de acuerdo a los roles al interior de la organización.

- ✓ **SEGURIDAD DE LA INFORMACIÓN**: Son todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información.

- ✓ **SERVIDOR:** Equipo de computación físico o virtual, en el cual funciona un software, cuyo propósito es proveer servicios a otros dispositivos dentro de la red.

- ✓ **SERVIDOR DE ALMACENAMIENTO:** Equipo servidor dotado con varios discos duros destinados a respaldar y compartir datos.

- ✓ **SISTEMA OPERATIVO (SO) U OPERATING SYSTEM (OS):** Programa o conjunto de programas que en un sistema informático gestiona los recursos de hardware y provee servicios a los programas de aplicación, ejecutándose en modo privilegiado respecto de los restantes.

6. COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección de la EFR, se compromete tanto con el desarrollo y la implementación de las políticas de Seguridad de la Información, como de la ejecución de las estrategias e instrumentos para su mejora continua, para lo cual, mantendrá un actuar permanente respecto a:

- ✓ Apoyar la implementación de la política de Seguridad de la Información en todas las áreas de la EFR
- ✓ Acompañar la revisión y aprobación de las políticas de Seguridad de la Información.
- ✓ Garantizar los recursos humanos, técnico y financieros necesarios para la correcta implementación de la política.
- ✓ Garantizar que la política se incorpore en la implementación del Sistema de Gestión de Seguridad de la Información.
- ✓ Garantizara una adecuada divulgación frente al cumplimiento de la política de Seguridad de la Información, así como su evaluación, monitoreo y control.

7. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

7.1. POLÍTICA PARA DISPOSITIVOS MÓVILES

- ✓ Se permite el uso de dispositivos móviles de conexión inalámbrica al interior de las instalaciones de la Empresa Férrea Regional SAS. únicamente para desarrollar y cumplir con los objetivos laborares y/o contractuales del personal, procurando que no se almacene en estos dispositivos información institucional.
- ✓ En el caso de asignar dispositivos móviles a administrativos o contratistas, estos son propiedad de la entidad, y los responsables de dichos equipos deberán velar por su adecuado uso, cuidado, mantenimiento y protección.
- ✓ Los medios de almacenamiento de estos dispositivos pueden ser protegidos tecnológicamente con medios de cifrado de datos o mediante cualquier otro mecanismo definido por la Dirección Administrativa Financiera (Área de Tecnologías), con el fin de evitar la interceptación y/o uso indebido de la información que en ellos se almacene.
- ✓ El funcionario asumirá los riesgos y costos asociados a la perdida, fuga o uso indebido de la información que se encontraba en los dispositivos extraviados, además del cumplimiento de las políticas y regulaciones vigentes por parte de la Dirección Administrativa y Financiera, concernientes a los costos del activo físico.
- ✓ La solicitud de conexión de dichos dispositivos a la red inalámbrica de la Empresa se realizará por intermedio de la mesa de ayuda de tecnología o por los funcionarios debidamente autorizados por el Área de Tecnologías de la Dirección Administrativa y Financiera.

- ✓ La autorización de retiro de las instalaciones de los dispositivos móviles se deberá regir por las regulaciones emitidas por el Área de Tecnologías de la Dirección Administrativa y Financiera, en lo concerniente a autorización de salida de elementos.

- ✓ Se prohíbe conectar a los perfiles de red institucionales dispositivos móviles de uso personal, salvo que exista autorización explícita emitida el Área de Tecnologías.

- ✓ Se prohíbe la entrada de teléfonos celulares y otros dispositivos móviles a los centros de datos y centros de cableado de la empresa, salvo que exista una autorización explícita emitida por el Área de Tecnologías

- ✓ La alta dirección de la empresa podrá exigir para determinadas reuniones la ausencia de dispositivos móviles, dispositivos de grabación y cualquier otro equipo electrónico que se especifique por razones confidencialidad o de evitar la interceptación y/o uso indebido de la información que en ellos se almacene.

- ✓ Para los visitantes y personal de apoyo que ingrese a la empresa y que requiera para sus funciones o servicios a prestar, el uso de alguno de estos dispositivos móviles, deben aplicarse las mismas restricciones de uso; adicionalmente, deberá estar siempre acompañado del responsable por parte de la empresa para esta visita, con el fin de evitar usos indebidos de las tecnologías.

7.2. POLÍTICA DE CONTROL DE ACCESO LÓGICO

- ✓ La Dirección Administrativa y Financiera (Área de Tecnologías) es la responsable de definir y suministrar los mecanismos de acceso lógico para la asignación de permisos y privilegios a los usuarios de acuerdo a sus funciones, términos contractuales y/o roles definidos al interior de la Empresa, así como la modificación los permisos y privilegios de los usuarios en los mecanismos y/o sistemas de autenticación definidos.

- ✓ El Área de Talento Humano es la encargada de notificar y dar los lineamientos para la creación, modificación y supresión de permisos y privilegios de usuarios.

- ✓ Se prohíbe el uso de las cuentas de usuario administrador local en la empresa, salvo en aquellos casos que estén debidamente justificados y autorizados.

- ✓ Los propietarios, responsables y/o custodios de los activos de información de la institución deben revisar periódicamente los derechos de acceso de los usuarios.

- ✓ Los propietarios y/o responsables de los activos deben informar inmediatamente sobre las novedades de los derechos de acceso lógico de los usuarios.

- ✓ Para la creación y administración de las credenciales de acceso institucionales, para empleados y contratistas, se deben adoptar los lineamientos establecidos por la Dirección Administrativa y Financiera (Área de Tecnologías).

- ✓ Los empleados y contratistas son los únicos responsables por la seguridad de sus credenciales de acceso (usuario y contraseña), las cuales son de uso exclusivo, único e intransferible.

7.3. POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS

- ✓ La Empresa Férrea Regional SAS. a través de la Dirección Administrativa (Área de Tecnologías) establecerá la implementación de los sistemas y técnicas criptográficas para la protección de la información, con base en los análisis de riesgos efectuados y con el fin de mantener la confidencialidad, integridad y autenticidad de la información.

- ✓ Cada dependencia de la Empresa Férrea Regional SAS., debe velar por tener una óptima administración de la información y debe implementar sistemas y técnicas criptográficas a la información catalogada como reservada o controlada, acorde a los lineamientos institucionales, con el fin de prevenir riesgos relacionados con la fuga de información durante su transmisión o almacenamiento teniendo en cuenta su nivel privada o simétrica dependiendo el caso.

- ✓ Se deben definir custodios o responsables de la información de carácter reservado en cada dependencia de la entidad.

- ✓ La Dirección Administrativa y Financiera (Área de Tecnologías) debe brindar el apoyo necesario a los funcionarios y contratistas, en el uso de las herramientas tecnológicas para protección de la información sensible, que debe ser cifrada.

- ✓ La Dirección Administrativa y Financiera (Área de Tecnologías), debe definir las herramientas necesarias para el cifrado de datos, de tal forma que preserve la confidencialidad, la integridad y el no-repudio en la transmisión de información sensible entre la comunidad y la Empresa Férrea Regional SAS.

- ✓ La Dirección Administrativa y Financiera (Área de Tecnologías), debe definir un procedimiento de gestión de claves, donde incluirán los métodos para la generación, longitud, eliminación y recuperación de claves en caso de pérdida, divulgación o daño.

- ✓ El procedimiento de gestión de claves debe tener en cuenta la fecha de finalización de contratos o de retiro de cada responsable del activo de información; de esta manera podrán desactivar, bloquear o eliminar los accesos no autorizados durante el periodo no laboral para que la información no corra ningún riesgo que afecte la continuidad de los procesos de la Empresa Férrea Regional SAS.

- ✓ Es responsabilidad del Área de Talento Humano y de la Oficina Asesora Jurídica informar al Área de Tecnologías sobre las novedades de retiro, con el fin de poder realizar las acciones de desactivación, bloqueo o eliminación de los respectivos accesos.

7.4. POLÍTICA DE TRANSFERENCIA E INTERCAMBIO DE INFORMACIÓN

- ✓ La Dirección Administrativa y Financiera (Área de Tecnologías) debe cumplir acciones de mejoramiento respecto a la seguridad de la información, principalmente respecto al uso de protocolos para realizar transferencia de información digital y/o física entre unidades, usuarios y terceras partes de la entidad.

- ✓ Los mensajes enviados a través de cualquier medio electrónico que contengan información pública, controlada o reservada, deben ir cifrados y estos deben ser conocidos solo por el emisor y por el receptor(es), del mensaje.

- ✓ Cada dependencia y/o supervisor de los contratos firmados con terceros, está en la necesidad de verificar la firma de los acuerdos de confidencialidad previo a la transferencia de información entre la Empresa Férrea Regional SAS. y sus proveedores y/o contratistas, en los casos que aplique.

- ✓ Las terceras partes implicadas se verán obligadas a firmar los formatos de confidencialidad aplicables. Estos formatos serán entregados por el supervisor del contrato para el caso de proveedores y contratistas, y por el Área de Talento Humano para los funcionarios. El formato hará parte del Sistema Integral de Gestión.

- ✓ Toda la información que se reciba o envié a través de impresoras, máquinas de fax u otros medios de reprografía y transmisión de datos, debe ser monitoreada por el funcionario o contratista que los esté utilizando y debe permanecer siempre sin ningún tipo de documentos o información clasificada como controlada o reservada.

- ✓ Toda la información verbal que sea intercambiada por conversaciones formales, atención de llamadas telefónicas y demás procesos que no dejen soportes físicos, debe cumplir con el protocolo de manejo y escalamiento de comunicaciones vigente para la Empresa.

- ✓ La Dirección Administrativa y Financiera (Área de Tecnologías) debe realizar capacitaciones y/o difundir los lineamientos institucionales para evitar que se traten temas de Empresa Férrea Regional SAS., en sitios públicos o escenarios no autorizados formalmente para la divulgación de información.

- ✓ Salvo casos de estricta necesidad y bajo previa autorización y/o recomendación de la Dirección Administrativa y Financiera (Área de Tecnologías), no se suscribirán o diligenciarán formularios electrónicos para uso personal o para medíos de investigación a través de internet, igualmente se debe impedir el diligenciamiento de los datos de ubicación física, teléfonos móviles, teléfonos fijos, estructura organizacional, divulgación

de cargos o información sensible de la Empresa Férrea regional SAS., cuando el personal se suscriba o diligencie formularios electrónicos para uso personal o para medíos de investigación a través de internet.

- ✓ La descarga de reportes a herramientas ofimáticas tipo hoja de cálculo será autorizada, pero el archivo de salida será enteramente identificable como un reporte diferente a los que el sistema genere en salidas de solo lectura.

- ✓ Los reportes extraídos claramente de los sistemas de información de la Empresa contaran con las siguientes características mínimas:

  - Deberán ser generados, almacenados y codificados según una fecha de corte claramente estipulada.

  - Tienen asignado un propietario, responsable o custodio y un validador de la información contenida.

  - El propietario es el único autorizado para su generación, difusión al interior de la entidad y el subsecuente archivo o salvaguarda.

- ✓ Los reportes oficiales utilizados para la certificación de totales, valores o listados, especialmente los dirigidos a entidades externas, organismos de inspección, control y/o vigilancia, deberán ser validados y firmados física o digitalmente por el responsable de la información, para esto la Empresa establecerá en sus procesos y procedimientos los propietarios, responsables y/o custodios para cada caso.

- ✓ El director de cada dependencia y/o jefe de oficina serán los responsables de definir los permisos de acceso a los dispositivos de almacenamiento central o SAN, como repositorio de información de la entidad.

- ✓ La Dirección Administrativa y Financiera (Área de Tecnologías) será la encargada de definir los mecanismos y lineamientos de uso de la unidad de almacenamiento SAN.

- ✓ La recepción de correspondencia rotulada como "Información Confidencial" exclusivamente podrá ser revisada y visualizada por el destinatario de los documentos.

- ✓ El envío de correspondencia rotulada como "Información Confidencial" solo podrá salir de la Empresa en medio impreso o digital con la expresa autorización del emisor.

- ✓ Cada dependencia está encargada de solicitar a la Dirección Administrativa y Financiera, (Área de Gestión Documental) la correspondencia rotulada como "No Confidencial" que no sea abierta por parte del grupo de correspondencia.

- ✓ Toda información clasificada como sensible o vulnerable que sea enviada por medios electrónicos, debe usar algoritmos de cifrado según los lineamientos de la Dirección Administrativa y Financiera (Área de Tecnologías) y la herramienta con la que cuenta la entidad.

- ✓ El funcionario encargado de la información de cada dependencia, es el responsable de velar por el cumplimiento de la clasificación, foliación y rotulación de los documentos, de conformidad con los términos ordenados por la Dirección Administrativa y Financiera (Área Gestión Documental) de la Empresa Férrea Regional SAS.

7.5. POLÍTICAS DE DESARROLLO SEGURO

- ✓ Las solicitudes de desarrollos nuevos o modificación de las aplicaciones actualmente instaladas que se encuentran en producción, deben ser tramitadas conforme a los procedimientos vigentes y estipulados para tal fin. De acuerdo al procedimiento, las solicitudes realizadas en el tiempo estipulado, serán sometidas a un proceso de verificación y posterior aprobación o rechazo de la solicitud. La sola radicación no implica aceptación y estará sujeta a un cronograma de desarrollo con prioridades según los objetivos misionales de la Empresa Férrea Regional SAS.

- ✓ La Dirección Administrativa y Financiera (Área de Tecnologías) es la única dependencia encargada de la realizar desarrollos dentro de la Empresa Férrea Regional SAS. y dará cumplimiento a los lineamientos de construcción de aplicaciones seguras adoptadas para la Empresa.

- ✓ Todo desarrollado será puesto en producción según las presentes políticas, los términos y condiciones de privacidad y el reglamento para el uso adecuado de las TICs.

- ✓ La Empresa Férrea Regional SAS apoyará la debida aplicación de los lineamientos de desarrollo facilitando los recursos, elementos y lugares de trabajo adecuados para el equipo de desarrollo de la entidad.

- ✓ Se prohíbe el acceso y/o uso de los recursos físicos y/o tecnológicos a personal no autorizado y en general, a los recursos asignados al grupo de desarrollo de por la Dirección Administrativa y Financiera (Área de Tecnologías). El intento de uso total o parcial del código fuente de las aplicaciones administradas y/o adquiridas por la Empresa, por parte de personal no autorizado queda expresamente prohibido.

- ✓ Con el fin de garantizar la seguridad, estabilidad y usabilidad de las soluciones, todos los desarrollos nuevos o modificaciones a desarrollos existentes, se deben realizar de conformidad con el procedimiento aprobado para ello.

- ✓ Las direcciones o jefaturas de la Empresa solicitantes de desarrollos nuevos o modificaciones a desarrollos ya existentes, deben asignar a funcionarios idóneos para colaborar en la realización y aprobación de los resultados de las pruebas.

- ✓ Las solicitudes de desarrollo o modificación de aplicaciones que no pueden ser atendidas por la Dirección Administrativa y Financiera (Área de Tecnologías) se regirán por el procedimiento de "Contratación de bienes y servicios" de la Empresa Férrea Regional SAS.

7.6. POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS

- ✓ El escritorio de trabajo de todos los funcionarios y contratistas la Empresa, debe permanecer completamente despejado y libre de documentos controlados y/o reservados a la vista del público.

- ✓ Todos los documentos controlados y/o reservados y en general, toda la documentación clasificada como "Información confidencial" debe permanecer guardados en un lugar seguro (archivadores con llaves), ya sea en un espacio físico o virtual, siempre que mantenga las debidas condiciones de almacenamiento y claves de acceso.

- ✓ El escritorio o la pantalla de inicio del computador, tableta, escritorio virtual o cualquier dispositivo que admita el acceso a información, debe permanecer libre de documentos, carpetas e íconos de acceso directo a archivos y/o carpetas que contengan documentos. En lo posible, sólo deben permanecer en la pantalla los íconos por defecto del sistema operativo instalado en el equipo.

- ✓ Todos los funcionarios y contratistas la Empresa son responsables de velar por la adecuada protección de la información física y lógica al ausentarse de su puesto de trabajo.

7.7. POLÍTICA DE GESTIÓN DE CAMBIOS

- ✓ Los recursos que se encuentran administrados por la Dirección Administrativa y Financiera (Área de Tecnologías), que son deben estar incluidos por un procedimiento de gestión de cambios y despliegue del servicio son: las aplicaciones de software que han sido desarrolladas internamente o desarrolladas externamente y entregadas formalmente para su administración, los equipos de cómputo misionales (servidores), las redes de telecomunicaciones locales, extendidas y externas, los manejadores de bases de datos institucionales y la información documentada de los servicios gestionados por esta gerencia.

- ✓ Cualquier modificación a las condiciones actuales de funcionamiento de los recursos administrados por la Dirección Administrativa y Financiera (Área de Tecnologías) y que

estén cobijados por el procedimiento de desarrollo de sistemas de información, serán considerados como cambios tecnológicos y por tanto, deben cumplir con los procedimientos y protocolos emitidos por el Área de Tecnología.

- ✓ La Dirección Administrativa y Financiera (Área de Tecnologías) determinará las fechas y responsables de efectuar la validación de condiciones y la correspondiente ejecución controlada del cambio.

- ✓ En casos de emergencia manifiesta, que estén afectando directamente la normal prestación de los servicios de la Empresa Férrea Regional SAS en cualquiera de sus dependencias, se podrán realizar cambios en la configuración de recursos y servicios de infraestructura tecnológica; sin que estos cambios sean susceptibles de revisión posterior por parte de la Dirección Administrativa y Financiera (Área de Tecnologías).

- ✓ La Empresa Férrea Regional SAS, propenderá porque los servicios tecnológicos que se encuentran tercerizados, cuenten con procedimientos y/o protocolos definidos para la gestión de cambios y despliegue del servicio sobre los servicios contratados.

7.8. POLÍTICAS DE BACKUPS O COPIAS DE SEGURIDAD

- ✓ La responsabilidad de la gestión de las copias de respaldo y la administración de los equipos de respaldo masivo de datos estará a cargo de la persona designada por el Director Administrativo y Financiero (Área de Tecnología); así el profesional (ingeniero de plataforma tecnológica) es el encargado de la administración de equipos de respaldo masivo de datos.

- ✓ El funcionario encargado de la administración de equipos de respaldo masivo de datos, velará por los backups y por la seguridad de los datos contenidos en ellos; asimismo como por su integridad, disponibilidad y confidencialidad y en su efecto el salva guarda de la información debe ser almacenados en un lugar que garantice su protección.

- ✓ Los medios de respaldo utilizados para efectuar las copias de seguridad en la Empresa Férrea Regional SAS, serán los definidos por el Director Administrativo y Financiero (Área de Tecnologías) en el procedimiento de copias de respaldo o aquel que lo supla.

- ✓ El responsable de la administración de equipos de respaldo masivo de datos, custodiará los respectivos medios de respaldo (y los datos contenidos en éstos) y serán quienes tengan acceso a ellos.

- ✓ Se hará respaldo a los archivos, aplicaciones, bases de datos y configuración de los sistemas operativos de los servidores calificados como críticos para la Empresa Férrea Regional SAS y contemplados en el Inventario de Servidores Críticos.

- ✓ Se incluye como información a respaldar, las configuraciones completas de los servidores locales o externos que estén en el inventario de la Empresa Férrea Regional SAS.

- ✓ La Dirección Administrativa y Financiera (Área de Tecnologías) será la responsable de definir los mecanismos adecuados para la ejecución de los respaldos de información, así como la periodicidad, etiquetado, lugar de archivo y el tiempo de retención de las copias.

- ✓ Para todos los casos de criticidad definidos en el Inventario de Servidores Críticos, será obligatorio contar con mínimo dos niveles de respaldo.

- ✓ La ejecución de las copias de seguridad debe realizarse en horas de poca o ninguna actividad laboral; por lo cual, la Dirección Administrativa y Financiera (Área de Tecnologías) será la responsable de precisar el horario de ejecución de éstas.

- ✓ En los casos en que el backup no finalice exitosamente en los tiempos establecidos, éste se relanzará después de evidenciado el fallo, en los tiempos determinados.

- ✓ Cuando sea preciso un respaldo por demanda de los servidores críticos, se debe requerir formalmente a través de correo electrónico por parte del personal autorizado, para informar mínimo con 24 horas de anterioridad sobre posibles interrupciones en el servicio a las personas afectadas.

- ✓ Todos los respaldos se revisarán con la periodicidad definida y se evidenciarán en la bitácora de backups.

- ✓ La comprobación periódica del estado de las copias se llevará a cabo con el fin de garantizar la disponibilidad e integridad de los datos almacenados. Los responsables de la administración de equipos de respaldo masivo de datos evidenciarán la comprobación periódica del estado de las copias de seguridad en el formato para pruebas periódicas de restauración de backups.

- ✓ Los equipos para el respaldo de información de la Empresa Férrea Regional SAS, deben estar ubicados en centros de datos (Datacenters) con las medidas de seguridad pertinentes, y tener contratos de soporte y mantenimiento regular vigentes.

- ✓ Los medios de almacenamiento de datos deben tener un manejo adecuado para mitigar la ocurrencia de daños físicos y por consiguiente la pérdida de la información.

7.9. POLÍTICA DE GESTIÓN, ADMINISTRACIÓN Y CONSERVACIÓN DOCUMENTAL

- ✓ La Empresa Férrea Regional SAS, está obligada a la creación, organización, preservación y control de los archivos, teniendo en cuenta los principios de procedencia, orden original, el ciclo vital de los documentos y la normatividad archivística.

- ✓ La Empresa Férrea Regional SAS, deberá garantizar los espacios y las instalaciones necesarias para la conservación de sus archivos. En los casos de construcción de edificios públicos, adecuación de espacios, adquisición o arrendamiento, deberán tenerse en cuenta las especificaciones técnicas existentes sobre áreas de archivos, como lo establece el Archivo General de la Nación.

- ✓ La documentación institucional es producto y propiedad de la Empresa Férrea Regional SAS, y ésta ejercerá el pleno control de sus recursos informativos. Los archivos públicos, por ser un bien de uso público, no son susceptibles de enajenación.

- ✓ La Empresa Férrea Regional SAS, podrá contratar con personas naturales o jurídicas, los servicios de custodia, organización, reprografía y conservación de documentos de archivo, esto teniendo en cuenta lo establecido por el Archivo General de la Nación.

- ✓ Los funcionarios y contratistas de la Empresa Férrea Regional SAS, al desvincularse de la Entidad, entregarán los documentos y archivos a su cargo debidamente organizados e inventariados, conforme a las normas y procedimientos que establezca la entidad, sin que ello implique exoneración de la responsabilidad a que haya lugar en caso de irregularidades.

- ✓ La Dirección Administrativa y Financiera tendrá la obligación de velar por la integridad, autenticidad, veracidad y fidelidad de la información de los documentos de archivo, liderando a través del Área de Gestión Documental la planeación, control, dirección, organización, capacitación, inspección o vigilancia, promoción y otras actividades involucradas en la gestión del ciclo de vida de la información, incluyendo la creación, mantenimiento (uso, almacenamiento, recuperación), y disposición, independientemente de los medios o soportes., así como la prestación de los servicios archivísticos en el archivo de gestión, central e histórico.

- ✓ Los funcionarios de archivo trabajarán sujetos a los más rigurosos principios de la ética profesional, y a lo dispuesto en la Constitución Política de Colombia y la Ley 594 del 2000 o Ley General de Archivos.

- ✓ La Dirección Administrativa y Financiera podrá incorporar tecnologías de avanzada en la administración, gestión, seguimiento, control y conservación de sus archivos, empleando cualquier medio técnico, electrónico, informático, óptico o telemático, siempre y cuando cumpla con los siguientes requisitos mínimos:

- Organización archivística de los documentos
- Realización de estudios técnicos para la adecuada toma de decisiones, teniendo en cuenta aspectos como la conservación física, las condiciones ambientales y operacionales, la seguridad, perdurabilidad y reproducción de la información contenida en estos soportes, así como el funcionamiento razonable del sistema a impactar en toda la Dirección Administrativa y Financiera.

✓ La Gestión Documental dentro del concepto de archivo total, comprende procesos tales como la producción o recepción, distribución, consulta, organización, recuperación y disposición final de los documentos.

✓ Será obligatorio para la Empresa Férrea Regional SAS, elaborar y adoptar las respectivas tablas de retención documental.

✓ Es obligación de la Dirección Administrativa y Financiera elaborar inventarios de los documentos que produzcan en ejercicio de las funciones de las diferentes direcciones y jefaturas, de manera que se asegure el control de los documentos en sus diferentes fases.

✓ Todas las personas tienen derecho a consultar los documentos de archivos públicos y a que se les expida copia de los mismos, siempre que dichos documentos no tengan carácter reservado conforme a la Constitución o a la ley; el costo de su reproducción estará fijado por el Acto Administrativo que expida la Empresa.

✓ La Empresa Férrea Regional SAS., garantizará el derecho a la intimidad personal y familiar, honra y buen nombre de las personas y demás derechos consagrados en la Constitución y las Leyes.

✓ Sólo por motivos legales, la Dirección Administrativa y Financiera podrá autorizar la salida temporal de los documentos de archivo, previa autorización de la gerencia de la Empres Férrea Regional SAS.

✓ La Dirección Administrativa y Financiera contará con instrumentos de planeación y control para la ejecución de las actividades del Sistema de Gestión Documental, mediante la elaboración de un Plan Institucional de Archivos, Programa de Gestión Documental Físico y/o Electrónico, Sistema Integrado de Conservación y demás instrumentos informacionales o de control.

✓ La Dirección Administrativa y Financiera establecerá los diferentes mecanismos, instrucciones o pasos a seguir en temas relacionados con la preservación y conservación a largo plazo de los archivos tanto físicos como electrónicos en cualquier soporte material.

7.10. POLÍTICA PARA TELETRABAJO

Esta política permite establecer lineamientos en la Gestión de Seguridad de la Información que tiene los funcionario y trabajadores oficiales de la EFR S.A.S. que se acogen a la modalidad de Teletrabajo para el uso, administración, consulta y operación de los servicios en las áreas de Teletrabajo

- ✓ La Dirección Administrativa y Financiera deberá establecer y divulgar el uso de la información y los servicios tecnológicos necesarios para garantizar el adecuado funcionamiento de la modalidad de Teletrabajo.

- ✓ Los computadores portátiles de propiedad de los colaboradores, se les debe realizar la verificación de los requerimientos tecnológicos del equipo a través del área de tecnologías de la Dirección Administrativa y Financiera y deberán cumplir con la política de control de acceso lógico.

- ✓ El área de Tecnología de la Dirección Administrativa y Financiera será la responsable de gestionar los riesgos de seguridad de la información que se identifiquen en la modalidad de Teletrabajo y así mismo proporcionar los controles que sirvan para mitigarlos.

- ✓ El área de Talento Humano de la Dirección Administrativa deberá verificar que los equipos personales de los colaboradores que realizan actividades de Teletrabajo cumplan con los lineamientos referentes a seguridad de la información, teniendo en cuenta lo enmarcado en la normativa y los procedimientos de Teletrabajo definidos por la empresa.

- ✓ El área de Tecnología de la Dirección Administrativa y Financiera deberá implementar los controles necesarios que permitan el acceso remoto a los servicios tecnológicos de la EFR S.A.S. a los colaboradores que realicen actividades en Teletrabajo, así mismo se deben tener en cuenta la revocación de servicios cuando el colaborador no continué realizando actividades de Teletrabajo. Los colaboradores en modo Teletrabajo o conectados vía VPN se les deberán aplicar los permisos de navegación y control de acceso limitado a su perfil o privilegios y se llevará registro de su conexión.

7.11. POLÍTICA DE SEGURIDAD DEL RECURSO HUMANO

- ✓ El área de Talento Humano de la Dirección Administrativa y Financiera deberá definir formalmente un mecanismo de verificación del personal en el momento en que se postula al cargo. Dicho mecanismo deberá incluir los aspectos legales y procedimentales de vinculación de la EFR S.A.S. y los que dicte la Función Pública.

- ✓ La Dirección de Contratación deberá definir una lista de verificación que contengan los aspectos necesarios para la revisión de los antecedentes del personal a contratar por prestación de servicios de acuerdo con lo que dicta la ley y la reglamentación vigente.

- ✓ La Dirección de Contratación en los procesos de selección de personal de planta y procesos contractuales deberán contener la autorización para el tratamiento de los datos personales de acuerdo con la política de tratamiento de datos personales de la EFR S.A.S y de acuerdo con lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios.

- ✓ Los documentos de verificación deberán reposar en la historia laboral o carpeta contractual del colaborador.

- ✓ El área de Talento Humano de la Dirección Administrativa y Financiera y la Dirección de Contratación deberán establecer los mecanismos o controles necesarios para proteger la confidencialidad y reserva de la información contenida en las historias laborales y expedientes contractuales.

7.12. POLÍTICA DE TERMINACIÓN O CAMBIO DE RESPONSABILIDADES DE EMPLEO

Lineamientos para las responsabilidades y deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo.

- ✓ El supervisor del contrato deberá recoger y custodiar la información de la EFR S.A.S. bajo la responsabilidad de los contratistas en caso de terminación anticipada, definitiva, temporal o cesión del contrato.

- ✓ El jefe inmediato o a quien delegue deberá recoger y custodiar la información de La EFR S.A.S. en el caso de retiro, investigación, inhabilidades, o cambio de funciones.

- ✓ El jefe inmediato o el supervisor del contrato deberán informar a la Dirección Administrativa y Financiera, cualquier novedad de desvinculación administrativa, laboral o contractual; una vez notificada la novedad la Dirección Administrativa y Financiera a través del área de tecnologías deberá proceder a la inactivación de los accesos, teniendo en cuenta los siguientes parámetros, atendiendo lo descrito en el procedimiento "Retiro de Personal" (PR-EFR-RHT-002):

    - Si el buzón pertenece a una cuenta de correo genérica (ejemplo: info@efr-cundinamarca.gov.co), a este se le deberá cambiar la contraseña inmediatamente y asignar nuevo responsable para evitar accesos no autorizados. • En caso de que el buzón sea objeto de investigación por parte de las autoridades competentes se les entregará en cadena de custodia una copia del buzón garantizando su integridad.
    - Se deben inactivar los accesos biométricos o de tarjetas de proximidad de los sistemas de control de acceso a las instalaciones de la EFR S.A.S.
    - Adicionalmente en desvinculación:

- Para el buzón de correo electrónico se creará una copia de respaldo una vez se dé por terminada la vinculación con la EFR S.A.S.
- Bajo ningún parámetro se podrán restablecer los accesos a estas cuentas; y no se podrán emitir correos ni notificaciones desde estos buzones.
- Se deben inactivar todos los accesos a los sistemas de información.
- Se debe solicitar la devolución del carné o cualquier distintivo de autenticación, que lo acredita como colaborador de la EFR S.A.S.
- Para los usuarios que manejen buzones genéricos deberán informarlo al supervisor para realizar la copia de información de esas cuentas adicionales.

7.13. POLÍTICA DE USO ACEPTABLE DE LOS ACTIVOS

Lineamientos para identificar, documentar e implementar las reglas para el uso aceptable de información.

✓ Los funcionarios, trabajadores oficiales y contratistas de prestación de servicios, deberán utilizar únicamente los aplicativos y equipos de cómputo autorizados por la Dirección Administrativa y Financiera.

✓ En caso de que el colaborador deba hacer uso de equipos ajenos a la EFR S.A.S., estos deberán cumplir con la legalidad del Software instalado, antivirus licenciado, actualizado y solo podrá conectarse a la red una vez esté avalado por la Dirección Administrativa y Financiera.

✓ El único servicio de correo electrónico autorizado para el manejo de la información institucional en la EFR S.A.S. es el que cuenta con el dominio efr-cundinamarca.gov.co.

✓ La EFR S.A.S. podrá denegar el acceso a los servicios de correo electrónico, inspeccionar, monitorear y/o cancelar un buzón de correo asignado en caso de posible desacato a las leyes, decretos o reglamentación interna de la empresa.

✓ Las firmas de documentos oficiales que se constituyan como activos de información de acuerdo a la tabla de retención documental o acto administrativo deben reposar en original o con firma digital, en ningún caso se debe utilizar firmas digitalizadas o escaneadas, salvo en aquellos que se autorice por la Gerencia General, indicando para qué fin y porqué medios.

✓ La EFR S.A.S. se reserva el derecho de monitorear los accesos y el uso de los buzones de correo institucionales, de todos sus funcionarios o contratistas, además podrá realizar copias de seguridad en cualquier momento, así como limitar el acceso temporal o definitivo, por solicitud expresa del ordenador(a) del gasto, supervisor del contrato, jefe inmediato, Gerencia General, Jefe de Oficina de Control Interno, así como a todos los servicios y accesos a sistemas de información de la empresa.

- ✓ Con el fin de mitigar la suplantación de correos electrónicos, se prohíbe suministrar acceso directo a los buzones de correo asignado a cada colaborador.

7.14. POLÍTICA DE DEVOLUCIÓN DE ACTIVOS

Todos los funcionarios, trabajadores oficiales y contratistas de prestación de servicios deberán devolver todos los activos de información de la EFR S.A.S. que se encuentren a su cargo al terminar su empleo, contrato o acuerdo.

- ✓ Los funcionarios, trabajadores oficiales y contratistas de prestación de servicios deberán devolver todos los activos de información de la EFR S.A.S. que se encuentran en su poder a la terminación de su empleo, contrato, convenio o acuerdo.

- ✓ Para el traslado de equipos de cómputo al almacén o a otros colaboradores, o baja de los inventarios por cualquier motivo, se deberá realizar un respaldo de la información que en él se encuentre. Posterior se debe gestionar el borrado de información de los dispositivos de cómputo, en los equipos que contengan medios de almacenamiento con el fin de propender que la información de la empresa contenida en estos medios no se pueda recuperar.

- ✓ Cuando se realice el traslado de equipos de cómputo a otros colaboradores, se deberá instalar de nuevo el sistema operativo y los programas de la línea base.

- ✓ La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro será el área de tecnologías de la Dirección Administrativa y Financiera. En tal virtud, toda reasignación de equipos deberá ajustarse al procedimiento de gestión de bienes de la empresa.

7.15. POLÍTICA DE GESTIÓN DE MEDIOS REMOVIBLES

La Dirección Administrativa y Financiera a través del área de tecnologías, establecerá los siguientes lineamientos:

- ✓ Un procedimiento para el uso de medios removibles.

- ✓ En ninguna circunstancia se dejará desatendido los medios de almacenamiento copias de seguridad de los sistemas de información.

- ✓ Los funcionarios que hagan uso de token para el desempeño de sus funciones u obligaciones deberán velar por la custodia y buen manejo de estos.

- ✓ Deberá proveer los métodos de cifrado de la información además de suministrar el software o herramienta utilizado para tal fin.

- ✓ Todo medio removible deberá ser escaneado mediante antivirus cada vez que se conecte a un equipo de la EFR S.A.S.

- ✓ Es responsabilidad de cada funcionario, trabajador oficial y/0 contratista de prestación de servicios tomar las medidas para la protección de la información contenida en medios removibles, para evitar acceso físico y lógico no autorizado, daños, pérdida de información o extravío de este.

- ✓ Se prohíbe el uso de medios removibles en lugares de acceso al público que contengan información reservada o clasificada de la EFR S.A.S.

- ✓ Para la disposición final de aparatos eléctricos y electrónicos como discos duros, se debe realizar la eliminación de la información a través de borrado seguro. Cuando un Disco Duro por su obsolescencia o daños irreparables se dañe y sea imposible realizar el borrado seguro se debe garantizar que la información no sea recuperable.

7.16. POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

Lineamientos para proteger a través de controles de acceso para que solo se permita el ingreso a personal autorizado a las áreas seguras.

- ✓ La Dirección Administrativa y Financiera deberá señalizar las áreas de acceso restringido.

- ✓ La Dirección Administrativa y Financiera deberá establecer un sistema de control de acceso a las instalaciones de la EFR S.A.S, así como a las áreas demarcadas con acceso restringido dentro de las oficinas.

- ✓ Las áreas de acceso restringido deben estar protegidas por los controles adecuados al ingreso a ellas.

- ✓ Todo el personal que ingrese al Centro de Datos deberá portar identificación visible.

- ✓ La Dirección Administrativa y Financiera deberá controlar que el Centro de Datos permanezca siempre con la puerta de acceso cerradas y con controles de seguridad que mitiguen el acceso a personal no autorizado.

- ✓ La Dirección Administrativa y Financiera deberá mantener en buen estado la infraestructura física del centro de datos, tales como el RACK, puerta, cerradura, techos, paredes, pisos, cielos rasos, entre otros.

- ✓ La Dirección Administrativa y Financiera mediante el área de tecnologías deberá realizar una revisión periódica del estado del centro de datos e informar cualquier anomalía presentada de la siguiente manera: daños en el rack y equipos activos de red, daños en infraestructura física la Gerencia General.

- ✓ La Dirección Administrativa y Financiera es el responsable del cumplimiento del protocolo de aseo en el centro de datos, así como deberán mantener libre de objetos o elementos que no sean propios en la operación.

7.17 POLÍTICA DE UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS

Lineamientos para los controles de ubicación y protección de los equipos teniendo en cuenta lo siguiente:

- ✓ Los equipos de cómputo e impresoras deberán estar situados y protegidos para reducir el riesgo contra amenazas ambientales y de acceso no autorizado.
- ✓ Los equipos de cómputo portátiles se deberán proteger mediante mecanismos que no permitan su pérdida.

7.18 POLÍTICA DE RETIRO DE ACTIVOS

Lineamientos para los controles de retiro de activos teniendo en cuenta lo siguiente:

- ✓ Se deberá registrar cuando los equipos de cómputo ingresan y se retiran de las instalaciones de la EFR S.A.S.
- ✓ Se deberá llevar un control en el almacén de los equipos cuando se asignan y cuando se hace su devolución, conforme al procedimiento de baja de inventarios.
- ✓ Todos los equipos de cómputo que vayan a ser reasignados o dados de baja, se les deberá realizar una copia de respaldo y gestionar el borrado de información de los dispositivos de cómputo.

7.19 POLÍTICA DE CONTROLES CONTRA CÓDIGOS MALICIOSOS

- ✓ El área de tecnologías de la Dirección Administrativa y Financiera deberá definir y documentar los controles para la detección, prevención y recuperación contra códigos maliciosos.
- ✓ El área de tecnologías de la Dirección Administrativa y Financiera deberá realizar campañas de concienciación a todos los funcionarios, trabajadores oficiales y contratistas de prestación de servicios en materia de protección, prevención y recuperación contra códigos maliciosos.
- ✓ El área de tecnologías de la Dirección Administrativa y Financiera deberá dictar los lineamientos para la instalación de software antivirus que brinde protección contra códigos maliciosos en todos los recursos informáticos de la EFR S.A.S. y asegurar que

estas herramientas no puedan ser deshabilitadas, así como mantenerlas actualizadas permanentemente.

- ✓ El área de tecnologías de la Dirección Administrativa y Financiera deberá realizar la actualización continua de la base de firmas y parches correspondiente del software de Antivirus y actualizaciones de sistema operativo. Todo mensaje sospechoso de procedencia desconocida deberá ser inmediatamente reportado a la Dirección Administrativa y Financiera para tomar las medidas de control necesarias.

7.20 POLÍTICA DE RESTRICCIONES SOBRE LA INSTALACIÓN DE SOFTWARE

- ✓ La Dirección Administrativa y Financiera a través del área de tecnologías deberá monitorear que la Infraestructura tecnológica de la EFR S.A.S no sea utilizada para actividades comerciales o para propósitos de entretenimiento, acceso o uso a material no autorizado.

- ✓ La Dirección Administrativa y Financiera a través del área de tecnologías deberá establecer que la infraestructura tecnológica sea usada exclusivamente para el desempeño laboral, o para el desarrollo de las funciones, actividades y obligaciones acordadas o contratadas.

- ✓ La Dirección Administrativa y Financiera a través del área de tecnologías deberá controlar la instalación y uso de máquinas virtuales y sólo podrá realizarse siempre y cuando sea una necesidad para el uso de las funciones o labor contratada y no viole derechos de autor.

- ✓ La Dirección Administrativa y Financiera a través del área de tecnologías podrá en cualquier momento realizar una inspección del software instalado en los equipos de cómputo.

- ✓ La Dirección Administrativa y Financiera designará y autorizará al personal para instalar, configurar y dar soporte a los equipos de cómputo de la EFR S.A.S

- ✓ La Dirección Administrativa y Financiera a través del área de tecnologías es la única dependencia autorizada para la administración del software, el cual no deberá ser copiado, suministrado a terceros o utilizado para fines personales.

8. APLICABILIDAD

El contenido de esta política aplica para todos los procesos y procedimientos de la Empresa Férrea Regional SAS, así como a todas las actuaciones administrativas que desarrollen las distintas direcciones y jefaturas de la Empresa, por intermedio de sus funcionarios o contratistas.