1. OBJETIVO

1.1. GENERAL

Establecer los lineamientos institucionales que orientan la gestión integral de la seguridad y privacidad de la información en la Empresa Férrea Regional S.A.S que promuevan el uso adecuado de los activos de información, garantizando su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, así como el cumplimiento de la normativa nacional e internacional aplicable, los requisitos contractuales y los principios de transparencia, ética pública y buenas prácticas de seguridad de la información.

1.2. OBJETIVOS ESPECÍFICOS

- Gestionar los activos de seguridad y privacidad de la información de la Empresa Férrea Regional S.A.S. en cuanto a su identificación, clasificación, tratamiento y protección, para preservar sus propiedades de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.
- Sensibilizar y capacitar al personal, contratistas y partes interesadas que requieran, fomentando una cultura de seguridad y privacidad de la información basada en el uso ético y responsable de la información institucional.
- Mantener en constante evaluación y mejora el Sistema de Gestión de Seguridad y privacidad de la Información, garantizando su actualización frente a cambios tecnológicos, normativos y de contexto organizacional.
- Fortalecer la capacidad institucional para prevenir, detectar y responder eficazmente ante incidentes o amenazas de seguridad y privacidad de la información, protegiendo la infraestructura tecnológica, los sistemas y los datos personales que son administrados por la Empresa Férrea Regional S.A.S.

2. ALCANCE

Esta política aplica a toda la entidad, incluyendo sus servidores públicos y contratistas que en el ejercicio de sus funciones accedan, procesen, trasmitan, custodien o administren información y activos tecnológicos de la Empresa Férrea Regional S.A.S.

3. DOCUMENTOS DE REFERENCIA

- Constitución Política de Colombia. Artículo 15.
- Ley 44 de 1993 "por la cual se modifica la Ley 23 de 1982 (que regula los derechos de autor)" y se modifica la Ley 29 de 1944.
- 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". Reglamentada parcialmente por los Decretos Nacionales 4124 de 2004, 1100 de 2014.
- 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. Parcialmente Reglamentada por el Decreto 1081 de 2015.
  vLey 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 884 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. Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015.
- 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 artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
- Decreto 1081 de 2015. "Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República."
- 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).
- CONPES 3854 de 2016 - Política de Seguridad Digital del Estado Colombiano.

- Decreto 1499 de 2017, Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- 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.
- Ley 2094 de 2021 "Por medio de la cual se reforma la ley 1952 de 2019 y se dictan otras disposiciones".
- Resolución 2277 de 2025. Expedida por el Ministerio TIC expidió la Resolución 02277 del 3 de junio de 2025, con la cual se actualiza el Modelo de Seguridad y Privacidad de la Información (MSPI), contenido en el Anexo 1 de la Resolución 500 de 2021.
- MA-EFR-GFT-001 Manual de Seguridad y Privacidad de la Información ISO/IEC 27001:2025 Sistemas de gestión de seguridad de la información.

4. RESPONSABILIDADES

COMITÉ INSTITUCIONAL DE GESTIÓN DE DESEMPEÑO

El comité Institucional de gestión y desempeño contará con subcomités técnicos como instancias encargadas de conocer y desarrollar técnicamente los temas y políticas asignadas. Para esto se cuenta con el subcomité técnico de seguridad digital que es la encargada de revisar lo asociado con los proyectos, las políticas y procesos que tengan relación con asuntos de TI y seguridad de la información, dentro del marco de las políticas de seguridad digital.

- Revisar la información presentada por el responsable del Sistema de gestión de seguridad y privacidad de la información - SGSPI.
- Aprobar las actualizaciones de la Política de Seguridad y Privacidad de la Información y de los documentos que la desarrollen.
- Hacer seguimiento al cumplimiento de los objetivos del SGSPI y su articulación con el SIG y el MIPG.
- Promover la cultura de seguridad y privacidad de la información en todos los niveles de la Empresa.

DIRECTOR ADMINISTRATIVO Y FINANCIERO

- Liderar el procedimiento de mantenimiento de bienes muebles e inmuebles.
- Elaborar para revisión de la Oficina asesora de planeación institucional las modificaciones que requiera el procedimiento.
- Aprobar y asegurar la implementación de la Política de Seguridad y Privacidad de la Información y los documentos que la soportan.
- Garantizar la asignación de los recursos humanos, tecnológicos y financieros necesarios para la operación del SGSPI.
- Velar por la protección de los activos de información y la aplicación efectiva de los controles de seguridad definidos.
- Supervisar la gestión de riesgos, incidentes y el cumplimiento de los objetivos del SGSPI.
- Presentar informes periódicos de avances, incidentes y resultados del SGSPI ante la Dirección General y el Comité Institucional de Gestión y Desempeño.
- Promover la cultura de seguridad y privacidad de la información dentro de la entidad.
- Autorizar la ejecución de auditorías y revisiones en materia de seguridad y privacidad de la información.

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

- Se encarga de coordinar la ejecución de las actividades derivadas de la planeación, implementación, revisión y mantenimiento del SGSI.
- Coordinar la implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad y Privacidad de la Información.
- Apoyar la identificación, análisis, evaluación y tratamiento de riesgos asociados a la seguridad y privacidad de la información, conforme a la metodología institucional alineada con la ISO/IEC 27005 y el MSPI del MinTIC.
- Monitorear el cumplimiento de políticas, procedimientos y controles del SGSPI.
- Coordinar la gestión de incidentes de seguridad de la información, incluyendo su análisis, registro, comunicación y cierre.
- Liderar las actividades de concienciación y capacitación en materia de seguridad y privacidad de la información.
- Acompañar los procesos de auditoría interna y externa del SGSPI, brindando soporte técnico y documental.
- Velar por la correcta gestión de accesos, privilegios, respaldos y controles técnicos de seguridad.
- Proponer planes de mejora y actualizaciones al SGSPI en función de los resultados de las auditorías o los cambios en la normatividad aplicable.
- Actuar como punto de contacto ante incidentes o requerimientos relacionados con la seguridad y privacidad de la información.

PROPIETARIO O DUEÑO DE LA INFORMACIÓN

- Son los líderes 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.
- Identificar, clasificar y mantener actualizados los activos de información de su dependencia.
- Asegurar la confidencialidad, integridad y disponibilidad de la información bajo su responsabilidad.
- Reportar oportunamente incidentes, vulnerabilidades o accesos no autorizados.
- Asegurar que los usuarios autorizados cumplan con las políticas y controles establecidos.

- Coordinar con el oficial de Seguridad y Privacidad la aplicación de controles o medidas de mitigación derivadas del análisis de riesgos.
- Participar en los procesos de auditoría, revisión y mejora continua del SGSPI.

CUSTODIO DE LA INFORMACIÓN

- Es el que tiene la responsabilidad de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido.
- Asegurar la protección física y lógica de la información y de los sistemas que la soportan.
- Implementar los controles técnicos y operativos necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información.
- Realizar copias de respaldo y verificar su recuperación periódica.
- Restringir los accesos conforme a los perfiles autorizados definidos por el propietario de la información.
- Informar de manera inmediata cualquier incidente o vulnerabilidad detectada en el manejo de la información o en los sistemas tecnológicos.
- Mantener actualizado el inventario de activos bajo su custodia.
- Velar por el cumplimiento de las políticas de seguridad, privacidad y uso aceptable de los recursos informáticos.
- Coordinar con el Líder de Seguridad y Privacidad de la Información la aplicación de controles correctivos o preventivos derivados del análisis de riesgos o auditorías.

USUARIO DE LA INFORMACIÓN

- Son todos los funcionarios, proveedores, contratistas, que, con la debida autorización del propietario de la información, pueden 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.
- Hacer uso responsable y ético de la información, los sistemas y los recursos tecnológicos de la entidad.
- Cumplir con las políticas, normas y procedimientos del SGSPI, incluyendo la política de uso aceptable de TIC.
- Respetar la clasificación de la información y no divulgar datos confidenciales o restringidos sin la debida autorización.
- Proteger sus credenciales de acceso (usuario y contraseña) y evitar el préstamo o uso compartido de estas.
- Reportar oportunamente al Líder de Seguridad y Privacidad de la Información cualquier incidente, anomalía o acceso indebido.
- Participar en los programas de capacitación y sensibilización sobre seguridad y privacidad de la información.
- Contribuir activamente a la mejora continua del SGSPI mediante la identificación de riesgos y oportunidades de mejora.
- Garantizar que la información que registre, modifique o elimine sea veraz, completa y oportuna.

OFICINA ASESORA DE PLANEACIÓN INSTITUCIONAL

- Revisar y validar las modificaciones al procedimiento así como de los formatos que se requieran para su ejecución, además de codificar y cambiar las versiones donde corresponda e incluirlos en el sistema de gestión.

PROFESIONAL ESPECIALIZADO A CARGO DEL PROCESO DE GESTIÓN DOCUMENTAL

- Implementar mecanismos de clasificación, custodia, conservación y disposición final de los documentos institucionales.
- Asegurar que los procedimientos de eliminación, digitalización, préstamo y acceso documental cumplan los principios de confidencialidad y trazabilidad.
- Apoyar el control del ciclo de vida de la información junto con el Líder de Seguridad y Privacidad.
- Proteger la integridad de los archivos físicos y digitales que contengan información sensible o crítica.

OFICINA DE CONTROL INTERNO

- Es el encargado de realizar revisiones regulares a la eficacia del proceso de gestión de recursos físicos y tecnológicos de la dirección administrativa y financiera.

5. TERMINOS Y DEFINICIONES

- **ACTIVO:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas.) que tenga valor para la Entidad (ISO/IEC 27000).

- **AMENAZA:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la Entidad. (ISO/IEC 27000).

- **ANÁLISIS DE RIESGO:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **AUDITORÍA:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de esta. (ISO/IEC 27000).

- **CONFIDENCIALIDAD:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

- **COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO:** Órgano colegiado encargado de realizar seguimiento al desempeño institucional y al cumplimiento del Sistema de Gestión de Seguridad y Privacidad de la Información, así como de aprobar las políticas, estrategias y planes asociados.
- **CONTROL:** Medida o acción implementada para modificar o mantener el riesgo dentro de niveles aceptables, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información.

- **CONTROL DE VERSIONES:** Mecanismo que permite asegurar la trazabilidad, actualización y aprobación formal de los documentos, procedimientos y configuraciones del Sistema de Gestión de Seguridad y Privacidad de la Información.
- **CONTINUIDAD DEL NEGOCIO:** Capacidad de la entidad para mantener la operación de sus procesos críticos y la prestación de servicios en niveles aceptables ante la ocurrencia de un evento disruptivo.
- **CUSTODIO DE LA INFORMACIÓN:** Persona o dependencia encargada de administrar y mantener los activos de información conforme a las políticas establecidas, garantizando su correcta protección, respaldo y disponibilidad.
- **DISPONIBILIDAD:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- **EVALUACIÓN DEL RIESGO:** Proceso mediante el cual se comparan los resultados del análisis de riesgos con los criterios establecidos para determinar si el riesgo es aceptable o requiere tratamiento.
- **GESTIÓN DEL CAMBIO:** Procedimiento formal para garantizar que cualquier modificación en los sistemas, procesos o configuraciones se realice de manera controlada, evaluando los impactos sobre la seguridad y privacidad de la información.
- **GESTIÓN DEL RIESGO:** Actividades coordinadas para dirigir y controlar una amenaza con relación a la probabilidad de ocurrencia.
- **GESTIÓN DE INCIDENTES:** Conjunto de procesos destinados a la detección, análisis, registro, respuesta y seguimiento de incidentes que afecten la seguridad o privacidad de la información.
- **INTEGRIDAD:** Propiedad de la información relativa a su exactitud y completitud.
- **INCIDENTE:** Violación o amenaza inminente a las políticas de seguridad digital, políticas de uso aceptable y/o prácticas de seguridad básicas.
- **OFICIAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN:** Servidor designado para coordinar, implementar y mantener el Sistema de Gestión de Seguridad y Privacidad de la Información, velando por el cumplimiento de las políticas, la gestión de riesgos y la respuesta ante incidentes.
- **PROPIETARIO DE LA INFORMACIÓN:** Persona o dependencia responsable de definir los requisitos de seguridad, clasificación, acceso, uso y protección de los activos de información bajo su control.
- **RECUPERACIÓN ANTE DESASTRES (DRP):** Conjunto de estrategias, procedimientos y recursos destinados a restaurar los sistemas tecnológicos y la información crítica tras una interrupción significativa.
- **RIESGO:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **SEGURIDAD DE LA INFORMACIÓN:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).
- **SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una entidad para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.
- **USUARIO DE LA INFORMACIÓN:** Persona autorizada para acceder, consultar o utilizar la información en el marco de sus funciones y bajo las normas de seguridad y confidencialidad definidas por la entidad.
- **TRATAMIENTO DEL RIESGO:** Proceso mediante el cual se seleccionan e implementan medidas para reducir, transferir, aceptar o eliminar el riesgo de seguridad de la información.
- **VULNERABILIDAD:** La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

6. CONDICIONES DE OPERACIÓN

6.1. POLÍTICA GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Empresa Férrea Regional S.A.S., se compromete a establecer, implementar, operar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad y Privacidad de la Información, asegurando la protección de los activos de información, servicios tecnológicos y datos personales para su custodia y administración.

Esta política aplica a toda la entidad, servidores públicos y contratistas, buscando la protección de los activos de seguridad de la información, a través del cumplimiento de los requisitos legales e institucionales, así como la generación e implementación de lineamientos para el óptimo tratamiento de la información y complementado con el diseño de controles, identificación y gestión de riesgos.

La Política de Seguridad de la Información estará determinada por las siguientes premisas:

- La gestión basada en riesgos y la aplicación de controles proporcionales a la criticidad de los activos.
- La adopción de medidas para prevenir, detectar, responder y recuperar ante incidentes de seguridad o privacidad.
- El cumplimiento de la normativa nacional e internacional aplicable en materia de seguridad digital, protección de datos personales y gobierno digital.
- El uso exclusivo de software y licencias legalmente adquiridas.
- Que cualquier auditoría de seguridad esté debidamente autorizada por la Oficina Asesora de Planeación con visto bueno de la Dirección General.
- La sensibilización y capacitación permanente del talento humano en temas de seguridad y privacidad.
- La mejora continua del SGSPI, alineado con la ISO/IEC 27001:2022, el MSPI del MinTIC y el MIPG

6.2. PRINCIPIOS RECTORES

La Política de Seguridad y Privacidad de la Información de la Empresa Férrea Regional S.A.S. se fundamenta en los siguientes principios:

- **Confidencialidad:** La información debe estar protegida frente a accesos, usos o divulgaciones no autorizadas.
- **Integridad:** La información debe conservar su exactitud, coherencia y completitud a lo largo de su ciclo de vida.
- **Disponibilidad:** La información y los sistemas deben estar accesibles y operativos para los usuarios autorizados cuando se requieran.
- **Autenticidad:** Se debe garantizar la veracidad e identidad de los usuarios, fuentes y sistemas que acceden o procesan la información.
- **Trazabilidad:** Debe mantenerse registro verificable de las acciones realizadas sobre los activos de información.
- **Legalidad:** Todas las acciones relacionadas con la gestión de información deben observar las normas y regulaciones aplicables.
- **Transparencia:** La entidad garantiza a los titulares de datos personales el acceso, conocimiento y control sobre el uso de su información.
- **Responsabilidad y rendición de cuentas:** Todo funcionario, contratista o tercero es responsable de proteger la información que gestiona.
- **Minimización y necesidad:** Solo se recolectará, procesará o conservará la información estrictamente necesaria para el cumplimiento de las funciones institucionales.
- **Proporcionalidad:** Las medidas y controles de seguridad deben corresponder al nivel de sensibilidad y riesgo asociado a la información tratada.

6.3. MANUAL DE SEGURIDAD DE LA INFORMACIÓN

La Empresa Férrea Regional S.A.S. reconoce que la información constituye uno de los activos más valiosos de la entidad, indispensable para el desarrollo de su misión institucional, el cumplimiento de sus objetivos estratégicos y la continuidad de sus operaciones.

En consecuencia, la Empresa establece el MA-EFR-GFT-003 Manual del Sistema de Gestión de Seguridad y Privacidad de la Información, como instrumento rector que define las políticas, lineamientos, responsabilidades, procedimientos y controles necesarios para garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información durante todo su ciclo de vida: creación, procesamiento, almacenamiento, transmisión, uso, archivo y eliminación.

6.3.1 ALCANCE Y OBLIGATORIEDAD

El Manual de Seguridad y Privacidad de la Información es de obligatorio cumplimiento para:

- Todos los servidores públicos y contratistas que conforman las diferentes áreas de la entidad y deberán clasificar la información que tengan bajo su custodia en alguna de las categorías establecidas.

6.3.2 CONFIDENCIALIDAD Y COMPROMISOS.

- Todos los contratistas, terceros y servidores públicos de la entidad deben suscribir el formato FR-EFR-GFT-016 Acuerdo de Confidencialidad y Debido Uso de la Información, el cual debe quedar debidamente resguardado en los expedientes contractuales de cada contratista o tercero y, en el caso de los servidores públicos, en sus respectivas historias laborales.

6.4. DIFUSIÓN, ACTUALIZACION SEGUIMIENTO, SANCIONES Y VIGENCIA

La Empresa Férrea Regional S.A.S comunicará todas las políticas, procedimientos 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.

La Empresa Férrea Regional S.A.S. fomentará una cultura institucional de seguridad y privacidad de la información, basada en la corresponsabilidad, la prevención y la concientización de todos los funcionarios, contratistas.

Para ello, se desarrollarán de forma periódica programas de formación, sensibilización y divulgación, orientados a fortalecer las competencias en materia de ciberseguridad, protección de datos personales, uso seguro de la información y cumplimiento de las políticas internas.

La Dirección Administrativa y Financiera, será responsable de incorporar la aplicación de la política de seguridad de la información en el plan de capacitación institucional y velar por la correcta inducción y reinducción de los funcionarios en materia de seguridad.

6.4.2 ACTUALIZACION

La presente Política de Seguridad y Privacidad de la Información será objeto de revisión al menos una vez al año, o cuando se presenten cambios significativos en la estructura organizacional, en los procesos institucionales, en la infraestructura tecnológica, en el contexto de amenazas o en el marco normativo aplicable.

6.4.3 SEGUIMIENTO

La Empresa Férrea Regional S.A.S. realizará auditorías internas y evaluaciones periódicas al proceso de recursos físicos y tecnológicos de la Dirección Administrativa y Financiera, con el fin de verificar el cumplimiento de esta política, la eficacia de los controles implementados el Modelo Integrado de Planeación y Gestión (MIPG) y la Política de Seguridad Digital del Estado.

Los resultados de las auditorías serán documentados y socializados con la alta dirección, quienes establecerán las acciones correctivas y de mejora requeridas para fortalecer el sistema.

6.4.4 SANCIONES

Cualquier violación a las políticas de seguridad de la información de la Empresa Férrea Regional S.A.S debe ser sancionada de acuerdo con el Reglamento Interno de Trabajo, a las normas, leyes y estatutos de la ley colombiana, así como la normativa atinente y supletoria, y apoyados en las leyes regulatorias de delitos informáticos de Colombia.

6.4.5 VIGENCIA

La presente política rige a partir de la fecha de su expedición y aprobación por parte del comité de Gestión y Desempeño.

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1	30/Ene/2020	Creación del documento.
2	18/Ene/2021	Actualización de vigencia
3	20/Nov/2023	Actualización de la política en marco general y segregación de las medias al manual de SGSPI
4	02/Dic/2024	Se estructuró la Política de Seguridad y Privacidad de la Información de la Empresa Férrea Regional S.A.S., alineada con la norma ISO/IEC 27001:2022, el Modelo de Seguridad y Privacidad de la Información (MSPI) versión 5 - MinTIC 2025, el MIPG y el MECI. Incluye definición de objetivos general y específicos, principios rectores, alcance, responsabilidades institucionales, condiciones de operación, lineamientos de cumplimiento, sanciones, difusión, control de cambios, seguimiento y mejora continua.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Darío Eduardo Muñeton **Cargo:** Contratista Dirección Administrativa y Financiera **Fecha:** 02/Dic/2025	**Nombre:** Deiryn Edith Reyes Medellín **Cargo:** Jefe Oficina Asesora de Planeación Institucional **Fecha:** 02/Dic/2025 **Nombre:** Yanny Lugdy Carrión Pedraza **Cargo:** Director Administrativo y Financiero **Fecha:** 02/Dic/2025	**Nombre:** Comité Institucional de Gestión y Desempeño **Cargo:** Ninguno **Fecha:** 02/Dic/2025