PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VIGENCIA 2021

EMPRESA FÉRREA REGIONAL S.A.S

BOGOTÁ, ENERO 2021

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

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA**	**NATURALEZA DEL CAMBIO**
1	06/11/2020	Creación del documento.
2	20/01/2021	Actualización del documento para la vigencia 2021

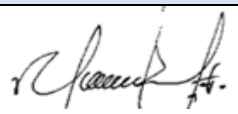
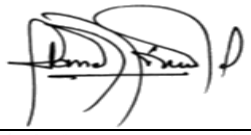
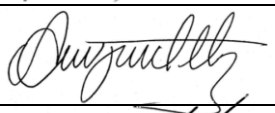
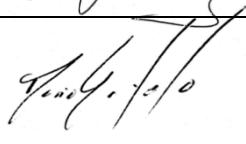
RESPONSABLE	CARGO	NOMBRE	FIRMA
APROBÓ	Gerente General	Jeimmy Villamil Buitrago	
REVISÓ	Subgerente General	Oscar Eduardo Rodríguez Lozano	
	Director Administrativo y Financiera	Iván Javier Gómez	
	Jefe Oficina Asesora de Planeación Institucional	Ana Judith Torres	
ELABORÓ	Contratista Dirección Administrativa y Financiera	Luis Darío Sotelo	

Tabla de Contenido

Introducción

El Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3. Principios. Define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera en el artículo 2.2.9.1.2.1 define la estructura de los elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales, los cuales son los elementos fundamentales de seguridad de la información, arquitectura y servicios para los ciudadanos digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

De igual manera el Decreto 2106 de 2019, por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública, en el parágrafo del artículo 16 indica que (…) Las autoridades deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones. (…).

Teniendo en cuenta lo anterior, se actualiza el Plan de Seguridad y Privacidad de la Información de la Empresa Férrea Regional S.A.S., de tal forma que el plan garantice la protección de la información y la privacidad de los datos de los ciudadanos y los funcionarios y contratistas de la Empresa, bajo los lineamientos de la legislación colombiana.

1. Objetivo del plan de seguridad y privacidad de la información.

Establecer las acciones estratégicas, encaminadas a fortalecer la seguridad y privacidad de la información de la Empresa Férrea Regional S.A.S, mediante la planeación de actividades para la mejora continua de la de seguridad de la información las cuáles serán gestionadas por los servidores públicos o contratistas de la EFR.

1.1. Objetivos específicos de la política de seguridad y privacidad de la información

Empresa Férrea Regional, para asegurar la dirección estratégica de la Entidad se establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, los cuales 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.

2. Política de seguridad de la información

La Empresa Férrea Regional S.A.S. por medio de su política de seguridad de la información, establece los lineamientos para proteger, preservar y administrar correctamente la información en la Entidad, junto con las tecnologías utilizadas 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 del plan estratégico de seguridad de la información

Aplica a toda la Empresa Férrea Regional SAS y sus involucrados, contratistas, proveedores, operadores y aquellas personas o terceros que, debido al cumplimiento de sus funciones y contratistas, compartan, utilicen, recolecten, procesen, intercambien o

consulten información, además de todas las personas relacionadas que accedan, ya sea interna o externamente a cualquier tipo de información de la Empresa, independientemente de su ubicación. El plan contempla el diseño, así como su implementación.

4. Términos y definiciones

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

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 organización. (ISO/IEC 27000).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25).

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera. También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.

Riesgo Positivo: Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.2

5. Plan de implementación del modelo de seguridad y privacidad en la información

El Plan de implementación para la dimensión de Seguridad y Privacidad de la Información comprende el siguiente cronograma:

Gestión	Actividades	Tareas	Responsable	Fecha Inicio	Fecha Final
Activos de Información	Definir lineamientos para el levantamiento de activos de información	Actualización de metodología e instrumento de levantamiento de activos de información	Área de Tecnologías	01/03/21	31/03/21
	Levantamiento Activos de Información	Elaborar y socializar la guía de activos de Información	Área de Tecnologías	01/03/21	31/03/21
		Validar activos de información de la vigencia anterior	Enlace de cada proceso; Área de Tecnologías	01/03/21	31/03/21

Gestión	Actividades	Tareas	Responsable	Fecha Inicio	Fecha Final
		Identificar nuevos activos de información en cada Dependencia	Enlace de cada proceso; Área de Tecnologías	01/03/21	31/03/21
		Realizar los instrumentos de activos de Información.	Enlace de cada proceso; Área de Tecnologías	01/04/21	30/04/21
	Registros activos de información ley 1712	Publicación del Registro Activos de Información en el sitio web de la Entidad.	Área de Tecnologías	1/09/21	22/09/21
Gestión de Riesgos	Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de Riesgos	Oficina de Riesgos y Seguridad Área de Tecnologías	01/03/21	31/03/21
	Sensibilización	Realizar la Implementación del plan de tratamiento de riesgos.	Oficina de Riesgos y Seguridad Área de Tecnologías	01/03/21	31/03/21
		Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información	Oficina de Riesgos y Seguridad Area de Tecnologías	03/05/21	31/05/21
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Oficina de Riesgos y Seguridad Area de Tecnologías	01/04/21	30/04/21
	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos identificados y planes de tratamiento	Oficina de Riesgos y Seguridad Área de Tecnologías	03/05/21	31/05/21
	Seguimiento Fase de Tratamiento	Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias	Oficina de Riesgos y Seguridad Área de Tecnologías	03/05/21	31/12/21

Gestión	Actividades	Tareas	Responsable	Fecha Inicio	Fecha Final
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Oficina de Riesgos y Seguridad Área de Tecnologías	03/05/21	31/12/21
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Oficina de Riesgos y Seguridad Área de Tecnologías	03/05/21	31/12/21
Gestión de Incidentes de Seguridad de la Información	Gestionar los incidentes de Seguridad de la Información identificado	Gestionar los incidentes de seguridad de la información de acuerdo con lo establecido en el procedimiento definido.	Área de Tecnologías	01/01/22	31/12/22
Plan de Cambio y Cultura de Seguridad y Privacidad de la Información , Seguridad Digital y Continuidad de la Operación	Elaborar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Elaborar el documento del Plan de Gestión de Cultura Organizacional	Área de Tecnologías	03/05/21	31/05/21
	Ejecutar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Implementar las estrategias del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficina Asesora de planeación Área de Tecnologías	01/01/22	31/12/22
Matriz de verificación de requisitos Legales de Seguridad de la	Creación de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Crear la Matriz de verificación de Requisitos legales de Seguridad de la Información	Oficina Asesora Jurídica Área de Tecnologías	01/01/22	31/12/22

Gestión	Actividades	Tareas	Responsable	Fecha Inicio	Fecha Final
Información	Revisión de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Evidenciar el cumplimiento de los Requisitos Legales de Seguridad de la Información	Oficina Asesora Jurídica Área de Tecnologías	01/06/22	31/12/22
Gobierno Digital	Gobierno Digital	Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información.	Área de Tecnologías	03/05/21	31/05/21
Protección de datos personales	Recolectar bases de datos	Elaborar y emitir un memorando para la recolección de bases de datos personales de acuerdo con los estándares emitidos por la SIC	Área de Tecnologías	03/05/21	31/05/21
	Revisión de bases de datos	Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos	Área de Tecnologías	03/05/21	31/12/21
	Registro y actualización de las bases de datos	Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información	Área de Tecnologías	03/05/21	31/12/21

6. Plan de Comunicaciones.

La Empresa Férrea Regional SAS definir un plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional, generando competencias y hábitos en todos los niveles, directivos, funcionarios, contratistas.

Este plan será ejecutado por la Dirección Administrativa y Financiera, bajo los parámetros de la Alta Dirección, y se aplicará a todas las áreas de la Entidad.

7. Indicadores de Gestión.

La Empresa Férrea Regional definirá un conjunto de indicadores que permitan medir la efectividad, la eficiencia y la eficacia en la gestión de la seguridad de la información, así

como el impacto de las acciones implementadas. Los indicadores deberán medir:

- Efectividad en los controles.
- Eficiencia de las acciones de seguridad de la información al interior de la entidad.
- Estado de seguridad de los procesos, que sirva de guía en las revisiones y la mejora continua de la gestión institucional.
- Comunicar valores de seguridad al interior de la entidad.

8. Privacidad de la información

Uno de los pilares del plan de seguridad y privacidad de la Información es garantizar un adecuado manejo de la información pública en poder de las entidades que recepcionan esta información, debido a que esta es el activo más importante para la toma de decisiones en cualquier organización; por ello, el plan debe asegurar que los procesos relacionados con los sistemas de información se complementen con el enfoque de “privacidad”, que permita la protección de los derechos a la intimidad y el buen nombre y la salvaguarda de secretos profesionales, industriales o de información privilegiada de particulares en poder de la administración cuando esta no sea sometida a reserva.

Es necesario para ello, incorporar a las acciones para la seguridad de la información un componente específico relacionado con la privacidad, a acciones o procesos como, la implementación de sistema de información que tenga la posibilidad de recolectar datos personales, el sistema de gestión documental de la Empresa, las directrices para la atención de las PQR´s y la transferencia de información a terceros (otras entidades o países).

9. Marco normativo

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1008 de 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- Decreto 620 de 2020. por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011, los literales e), j) y literal a) del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9° del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

10. Requisitos técnicos

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad

de la información.

- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.