	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión: 04</b>
		<b>Fecha: 28/01/2022</b>
	PL-EFR-GTI-002	<b>Página 1 de 9</b>

# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VIGENCIA 2022

## EMPRESA FÉRREA REGIONAL S.A.S

BOGOTÁ, ENERO 2022


---



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](http://www.efr-cundinamarca.gov.co)

 @efrcundinamarca
  @efrcundinamarca
  @efrcundinamarca

	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión: 04</b>
		<b>Fecha: 28/01/2022</b>
	PL-EFR-GTI-002	<b>Página 2 de 9</b>


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
3	02/12/2021	Actualización según los recursos técnicos, humanos y financieros disponibles para la ejecución de las actividades del plan.
4	28/01/2022	Actualización del documento para la vigencia 2022

RESPONSABLE	CARGO	NOMBRE	FIRMA
<b>APROBÓ</b>	Subgerente General	Oscar Eduardo Rodríguez Lozano	
<b>REVISÓ</b>	Directora Administrativa y Financiera (E)	Blanca Patricia Gómez Moreno	
<b>REVISÓ</b>	Contratista Dirección Administrativa y Financiera	Ronal Giovanni Quecan Fetecua	
<b>ELABORÓ</b>	Jefe Oficina Asesora de Planeación Institucional	Esteban Mancera Orjuela	

	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión: 04</b>
		<b>Fecha: 28/01/2022</b>
	PL-EFR-GTI-002	<b>Página 3 de 9</b>

### Tabla de Contenido

Tabla de Contenido.....	3
Introducción .....	4
1. Objetivo del plan de seguridad y privacidad de la información.....	5
1.1. Objetivos específicos de la política de seguridad y privacidad de la información .....	5
2. Alcance del plan de seguridad de la información .....	5
3. Marco normativo .....	5
4. Términos y definiciones.....	6
5. Plan de implementación del modelo de seguridad y privacidad en la información.....	7
6. Indicadores de Gestión. ....	9


	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	Versión: 04
		Fecha: <b>28/01/2022</b>
	PL-EFR-GTI-002	Página 4 de 9

## Introducción

El Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, define la seguridad de la información como un principio de la Política de Gobierno Digital, con componentes y habilitadores transversales, que permiten mejorar la gestión pública y la relación del estado con los ciudadanos.

Los lineamientos de seguridad de la información buscan que las entidades públicas preserven la confidencialidad, integridad, disponibilidad y privacidad de los datos en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información.

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 se garantice la protección de la información y la privacidad de los datos de los ciudadanos, los funcionarios y contratistas de la Empresa, bajo los lineamientos de la legislación colombiana.

	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión: 04</b>
		<b>Fecha: 28/01/2022</b>
	PL-EFR-GTI-002	<b>Página 5 de 9</b>

## 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 en la Empresa Férrea Regional S.A.S, mediante la preservación de la confidencialidad, integridad y disponibilidad de la información.

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


- Garantizar la disponibilidad de la información que la EFR requiere para su operación.
- Proteger los activos de información de manera que se garantice su integridad.
- Establecer protocolos que promuevan la confidencialidad de la información que se considere clasificada o reservada.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y demás partes interesadas de la Empresa Férrea Regional SAS.
- Garantizar la continuidad del negocio frente a incidentes.

## 2. Alcance del plan de seguridad de la información

Aplica a toda la Empresa Férrea Regional SAS y sus grupos de valor: contratistas, proveedores, operadores y aquellos terceros que, debido al cumplimiento de sus obligaciones compartan, utilicen, recolecten, procesen, intercambien o consulten información.

## 3. 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.

	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión: 04</b>
		<b>Fecha: 28/01/2022</b>
	PL-EFR-GTI-002	<b>Página 6 de 9</b>

- 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.

#### 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

	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión: 04</b>
		<b>Fecha:</b> <b>28/01/2022</b>
	PL-EFR-GTI-002	<b>Página 7 de 9</b>

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.

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

Actividad	Responsable	Entregable / producto	Programación 2022			
			Trim 1	Trim 2	Trim 3	Trim 4
Actualización del Diagnóstico del Modelo de Seguridad y Privacidad de la Información.	Dirección administrativa y financiera / Oficina de Planeación	Diagnostico actualizado		X		
Actualizar contexto de la organización con los factores externos e interno que puedan afectar la seguridad de la información	Dirección administrativa y financiera/ Oficina de Planeación	Contexto actualizado		X		



**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Versión: 04


Fecha:  
28/01/2022

PL-EFR-GTI-002

Página 8 de 9

Actividad	Responsable	Entregable / producto	Programación 2022			
			Trim 1	Trim 2	Trim 3	Trim 4
Adoptar política de seguridad de la información y los objetivos que la materializan	Dirección administrativa y financiera / Oficina de Planeación	Política y objetivos definidos				X
Documentar alcance del sistema de gestión de seguridad de la información	Dirección administrativa y financiera / Oficina de Planeación	Alcance documentado		X	X	X
Identificación, clasificación, valoración y asignación de responsables de Activos de Información (Software, Hardware, Redes y Telecomunicaciones, Servicios de Tecnologías de Información y de las Comunicaciones, Soportes, Servicios de Tecnologías de Información y de las Comunicaciones contratados)	Dirección administrativa y financiera	Inventario de activos de información		X		
Identificación, valoración y tratamiento de riesgos de Seguridad Digital	Dirección administrativa y financiera / Oficina de Planeación	Matriz de riesgos de seguridad digital			X	
Implementación de Controles de Seguridad Informática.	Dirección administrativa y financiera	Controles implementados			X	X
Socialización sobre la gestión de riesgos de seguridad digital y sus controles	Dirección administrativa y financiera / Oficina de Planeación	Listados de asistencia		X	X	
Elaborar procedimiento para la atención de incidentes de seguridad de la información	Dirección administrativa y financiera / Oficina de Planeación	Procedimiento implementado			X	
Gestionar los incidentes de seguridad de la información según el procedimiento	Dirección administrativa y financiera / Oficina de Planeación	Incidentes atendidos		X	X	X
Realizar evaluación de vulnerabilidades informáticas	Dirección administrativa y financiera / Oficina de Planeación	Informe de vulnerabilidades		X	X	



	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>Versión: 04</b>
		<b>Fecha: 28/01/2022</b>
	PL-EFR-GTI-002	<b>Página 9 de 9</b>

## 6. 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.