CONTROL DE CAMBIOS		
VERSIÓN	**FECHA**	**NATURALEZA DEL CAMBIO**
1	30/01/2020	Creación del documento.
2	18/01/2021	Actualización de vigencia
3	02/12/2021	Actualización del plan según los recursos humanos, técnicos y financieros disponibles.
4	25/01/2022	Actualización del documento para la vigencia 2022.
5	23/01/2023	Actualización del documento para la vigencia 2023. Se actualiza el código del documento de PL-EFR-GTI-003 por PL-EFR-GFT-003 dado el cambio en el mapa de procesos.
6	24/01/2023	Actualización del documento para la vigencia 2024. Se actualiza la identificación, valoración, evaluación y apetito del riesgo, de acuerdo al guía de Administración del Riesgo de la DAFP en su versión 6.
7	30/01/2025	Actualización del documento para la vigencia 2025

RESPONSABLE	CARGO	NOMBRE	FIRMA
APROBÓ	Comité Institucional de gestión y desempeño		
REVISÓ	Directora Administrativa y Financiera	Yanny Carrión Pedraza	Firmado Electrónicamente
	Jefe Oficina Asesora de Planeación Institucional	Deiryn Edith Reyes Medellín	Firmado Electrónicamente
	Jefe Oficina de Riesgos y Seguridad	Yeiny Alexandra Cubillos	Firmado Electrónicamente
ELABORÓ	Contratista Dirección Administrativa y Financiera	Carlos Andrés Monroy Barreto	Firmado Electrónicamente
	Contratista Oficina de Riesgos y Seguridad	María Alejandra Castiblanco	Firmado Electrónicamente

TABLA DE CONTENIDO

INTRODUCCIÓN

El propósito del Plan de tratamiento de riesgos y seguridad de la información es apoyar la implementación de controles que permitan a la Empresa reducir la probabilidad y el impacto de eventos que puedan afectar la seguridad de los activos de información.

La Empresa Férrea Regional S.A.S analiza los riesgos de los activos de información, que permite entender de una manera efectiva y eficiente los riesgos de pérdida de confidencialidad, integridad y disponibilidad sobre cada uno de los activos.

1. OBJETIVO GENERAL

Establecer y desarrollar un plan de acción integral para la gestión de riesgos de seguridad de la información y digital, con el objetivo primordial de preservar la integridad, confidencialidad y disponibilidad de los activos de información institucional.

1.1. OBJETIVOS ESPECÍFICOS

- Identificar los riesgos asociados con cada uno de los activos de información, enfocándonos en cómo estos riesgos pueden afectar la confidencialidad, integridad y disponibilidad de la información.
- Desarrollar e implementar una serie de controles personalizados y efectivos, mediante planes detallados y específicos.
- Estos controles estarán diseñados para abordar y mitigar los riesgos críticos identificados asegurando la protección de los activos de información.
- Implementar estrategias proactivas para reducir la probabilidad de que los riesgos identificados afecten a los activos de información.
- Realizar campañas de formación y concienciación de los funcionarios sobre seguridad de la información.

2. ALCANCE

Este plan se enfocará en la identificación, evaluación y mitigación de riesgos asociados a los activos de información de la Empresa Férrea Regional, también se incorporarán prácticas continuas de monitoreo y revisión para adaptarse a las cambiantes amenazas de seguridad y garantizar una protección efectiva de la información.

3. DOCUMENTACIÓN DE REFERENCIA

- **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 2018:** Por el cual se establecen los lineamientos generales de la

política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015,

- Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

- **CONPES 3854 de 2016**: Política Nacional de Seguridad Digital

- **Ley 1474 de 2011**: por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

- **Decreto 2641 de 2012:** por medio del cual se reglamentan los artículos 73 y 76 de la Ley 1474 de 2011, señalando como metodología para diseñar y hacer seguimiento a la estrategia de lucha contra la corrupción y de atención al ciudadano, la contenida en el documento "Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano".

- Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP 2022 V6

4. TÉRMINOS Y DEFINICIONES

- **ACEPTACIÓN DEL RIESGO:** Decisión informada de tomar un riesgo particular.

- **AMENAZA:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

- **ANÁLISIS DE RIESGO:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de este.

- **CONTROL:** Medida que modifica el riesgo.

- **EVALUACIÓN DE RIESGOS**: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

- **GESTIÓN DEL RIESGO:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

- **IMPACTO:** consecuencias que puede ocasionar a la organización la materialización del riesgo.

- **INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN**: Evento único o serie de

eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

- **PROBABILIDAD:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

- **PROPIETARIO DEL RIESGO:** Persona o Entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

- **RIESGO:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

- **RIESGO RESIDUAL**: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

- **RIESGO DE SEGURIDAD DE LA INFORMACIÓN:** Probabilidad de ocurrencia de un evento que genere un impacto sobre la Confidencialidad, Integridad y Disponibilidad de la Información.

- **VALORACIÓN DEL RIESGO:** Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

- **TRATAMIENTO DEL RIESGO:** Proceso para modificar el riesgo.

- **TRIADA DE LA INFORMACIÓN:** Conjunto de las propiedades derivadas de la Confidencialidad, Integridad y Disponibilidad de la Información.

- **VULNERABILIDAD:** Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

5. CONDICIONES DE OPERACIÓN

La técnica de análisis de riesgo para activos de información nos permite desde un punto de vista orientado al negocio, comprender claramente los riesgos sobre los activos de información a los que puede estar expuesta la Empresa Férrea Regional SAS.

Las técnicas tradicionales de análisis están encaminadas a identificar los riesgos específicos asociados a los activos y complementar esté proceso en la medida de lo posible con la identificación de puntos críticos de fallas, análisis de disponibilidad, análisis de vulnerabilidad, análisis de confiabilidad y árboles de falla.

La gestión del riesgo dentro de la seguridad de la información se enmarca en el ciclo de planear, hacer, verificar y actuar.

5.1. IDENTIFICACIÓN DE LOS ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN

Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como:

- Aplicaciones de la organización
- Servicios web
- Redes
- Información física o digital
- Tecnologías de información TI
- Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital

El líder de cada área desempeñará un papel clave en este proceso, será su responsabilidad no solo identificar y clasificar los activos de información, sino también realizar una priorización cuidadosa de aquellos activos que tengan una calificación de riesgo en nivel alto

5.2. IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS

La identificación de los riesgos de seguridad de la información implica la necesidad de determinar los activos de información asociados a los procesos, siguiendo las pautas establecidas en el Manual de Gestión de Riesgos de Seguridad y Privacidad de la Información.

Esta práctica permite identificar de manera efectiva los riesgos inherentes que están vinculados a esos activos, abarcando aspectos cruciales para la salvaguarda de la integridad, confidencialidad y disponibilidad de la información.

Cada riesgo debe estar vinculado con el conjunto de activos correspondiente, ya sea el grupo de activos en su totalidad o activos específicos asociados al proceso. Es esencial realizar un análisis integral, considerando de manera conjunta las posibles amenazas y vulnerabilidades que podrían dar lugar a la materialización de dichos riesgos. Este enfoque garantiza una

evaluación exhaustiva y precisa de los factores que pueden afectar la seguridad de los activos, permitiendo así la implementación de medidas preventivas y correctivas adecuadas.

Por otro lado, para la valoración de los riesgos se tendrá en cuenta la determinación de la probabilidad de ocurrencia, se encuentra directamente vinculada a la exposición al riesgo inherente a la actividad o proceso bajo consideración. De manera más específica, la probabilidad inherente se define como la frecuencia con la que se atraviesa el punto de riesgo en el transcurso de un año. Este enfoque permite cuantificar y evaluar con mayor precisión la incidencia potencial de los riesgos en el período temporal mencionado, proporcionando así una base sólida para la toma de decisiones informadas y la implementación de estrategias de gestión de riesgos eficaces.

La exposición al riesgo está directamente ligada a la naturaleza del proceso o actividad que se encuentra bajo análisis, se relaciona con la frecuencia con la que se atraviesa el punto de riesgo durante el periodo de un año. En la siguiente tabla se detallan criterios específicos que sirven para definir el nivel de probabilidad asociado a cada situación.

Estos criterios proporcionan un marco de referencia claro y objetivo, permitiendo una clasificación precisa de la probabilidad inherente a cada riesgo identificado. Este enfoque estructurado facilita la comprensión y comunicación efectiva de los niveles de probabilidad en el contexto del análisis de riesgos.

Criterios para definir el nivel de probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Versión 6

El impacto de un riesgo se refiere a las consecuencias y efectos adversos que la materialización de dicho riesgo podría tener en un sistema, proceso, proyecto o entidad específica. Este concepto abarca una variedad de aspectos, incluyendo la confidencialidad, integridad y disponibilidad de la información, así como otros elementos críticos para el funcionamiento eficiente y seguro de la entidad o sistema en consideración.

La determinación del impacto implica evaluar la magnitud de los daños o pérdidas potenciales en términos de objetivos, metas, recursos y activos afectados.

La clasificación del impacto puede variar desde consecuencias leves o moderadas hasta impactos severos que pueden afectar significativamente la operatividad y la capacidad de la entidad para cumplir con sus objetivos. La comprensión del impacto es esencial para una adecuada gestión de riesgos, ya que ayuda a priorizar acciones y asignar recursos de manera efectiva para mitigar o manejar los riesgos identificados.

Criterios para definir el nivel de impacto

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Versión 6

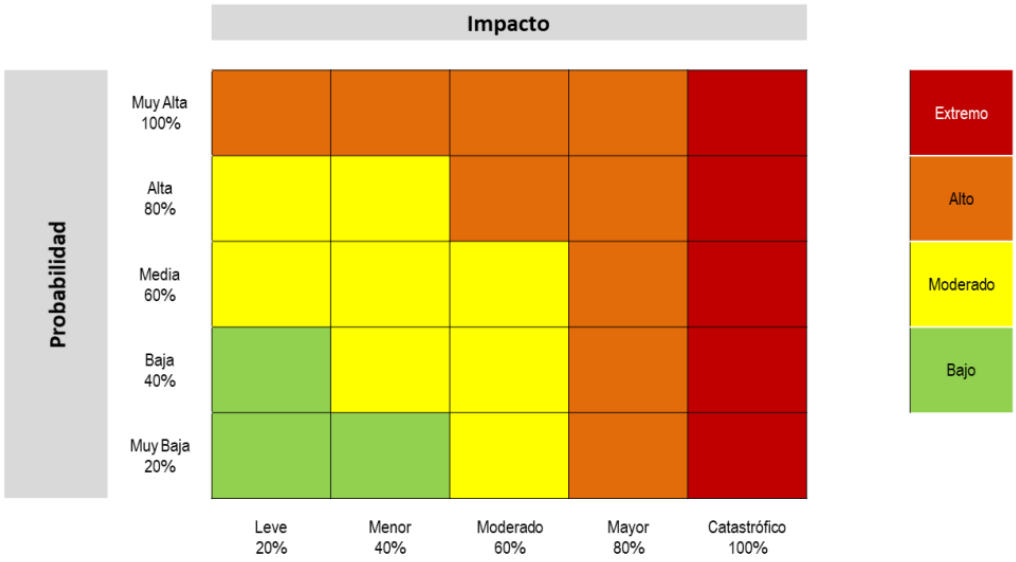
5.3. EVALUACIÓN DEL RIESGO

A partir de la evaluación de la probabilidad de ocurrencia de un riesgo y sus consecuencias o impacto, nuestro objetivo es identificar la zona de riesgo inicial, conocida como *"Riesgo Inherente".* Este proceso implica determinar los niveles de severidad mediante la combinación de la probabilidad y el impacto asociado a cada riesgo.

En este contexto, se establecen cuatro zonas de severidad en la matriz de calor, la matriz representa visualmente la relación entre la probabilidad y el impacto, clasificando los riesgos en distintas categorías según la magnitud de su impacto potencial y la probabilidad de su ocurrencia. Este enfoque facilita la identificación de riesgos críticos y permite la asignación de recursos de manera más efectiva, priorizando aquellos que poseen una combinación más alta

de probabilidad e impacto, y requieren una atención prioritaria en las estrategias de gestión de riesgos.

Matriz de Calor (Niveles de Severidad del riesgo)



Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Versión 6

5.4. APETITO DEL RIESGO

- NIVEL BAJO: En este nivel, se optará por ACEPTAR el riesgo y se gestionará mediante las actividades inherentes al proceso, con un enfoque en su control y registro de avance. La presentación detallada de estos controles y avances se incluirá en el Informe de Desempeño semestral, garantizando una transparencia y seguimiento continuo.

- NIVEL MODERADO: Para riesgos de nivel moderado, se implementarán acciones de control preventivo con el objetivo de REDUCIR la probabilidad de ocurrencia. Estas acciones se administrarán mediante un seguimiento trimestral, registrando detalladamente los progresos para un monitoreo eficiente, mediante un plan de acción que cuente con responsable, fecha de implementación y fecha de seguimiento.

- NIVEL MAYOR O ALTO: En este nivel, se establecerán acciones de control preventivo para REDUCIR tanto la probabilidad como la materialización del riesgo. La gestión de estos riesgos se llevará a cabo con un seguimiento trimestral, donde se debe realizar un plan de acción que cuente con responsable, fecha de implementación y fecha de seguimiento.

- NIVEL EXTREMO: Ante riesgos de nivel extremo, se implementarán acciones integrales, que incluyen controles preventivos y detectivos para REDUCIR la materialización del riesgo. Además, se considerará la posibilidad de EVITAR el riesgo mediante la eliminación o la no continuación de las actividades propensas al riesgo. Asimismo, se explorará la opción de TRANSFERIR o COMPARTIR una parte del riesgo para reducir su probabilidad o impacto. El monitoreo trimestral será crucial en este nivel, asegurando una vigilancia constante para evitar a toda costa la materialización de estos riesgos por parte de los procesos involucrados. Este enfoque integral busca minimizar los impactos negativos en la organización y garantizar una gestión efectiva de los riesgos más críticos.

5.5. CRONOGRAMA

Para dar cumplimiento al ciclo de gestión del riesgo, se establecen las siguientes acciones de implementación del plan de tratamiento a riesgos de seguridad de la información.

Actividad	Responsable	Entregable / producto	Programación 2025			
			Trim 1	Trim 2	Trim 3	Trim 4
Capacitación sobre la gestión de riesgos de seguridad digital y sus controles	Gestión de Recursos físicos y tecnológicos /Oficina de riesgos y seguridad	Listados de asistencia	X	X	X	X
Identificar, analizar y evaluar los riesgos de aquellos activos de información con criticidad alta	Dirección administrativa y financiera	Matriz actualizada de riesgos de seguridad	X	X		
Establecer controles, indicadores y plan de tratamiento sobre los riesgos	Dirección administrativa y financiera	Matriz de controles, fichas de indicadores y plan de tratamiento		X		
Socializar y aprobar los riesgos identificados por cada uno de los líderes de área	Dirección administrativa y financiera / Lideres de área	Informe de entrega con la respectiva matriz de riesgos		X		
Realizar seguimiento a los planes de tratamiento de riesgos de seguridad de la información establecidos por	Dirección administrativa y	Seguimiento a la implementación del plan de			X	X

Actividad	Responsable	Entregable / producto	Programación 2025			
			Trim 1	Trim 2	Trim 3	Trim 4
cada uno de los líderes de las áreas, con sus respectivas evidencias.	financiera / Lideres de área	tratamiento de riesgos (verificación de evidencias)				
Identificar oportunidades de mejora conforme los resultados de la evaluación del riesgo residual	Dirección administrativa y financiera	Oportunidad de mejora documentada				X

6. INDICADORES

INDICADORES	
CUMPLIMIENTO	(Número de actividades ejecutadas en el trimestre / Número de actividades programadas en el trimestre) x 100