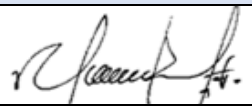
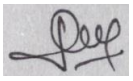
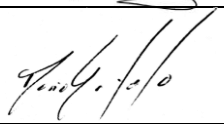
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN VIGENCIA 2021

EMPRESA FÉRREA REGIONAL S.A.S

BOGOTÁ, ENERO 2021

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA**	**NATURALEZA DEL CAMBIO**
1	30/01/2020	Creación del documento.
2	18/01/2021	Actualización de vigencia

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	Darío Sotelo	
	Contratista Oficina Asesora de Planeación	Katherine Rodríguez C.	

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 disminuir la probabilidad y el impacto de materialización de este tipo de riesgos, con el fin de preservar la seguridad e integridad de los activos de información de la entidad. El plan es de competencia de la Dirección Administrativa y Financiera a través del proceso de gestión de recursos tecnológicos y seguridad de la 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, definidos como parte de su alcance.

Formalizar de manera eficaz la seguridad de la información y riesgos de seguridad digital de los sistemas de información de la entidad, así como en los activos que participan en sus procesos y que se encuentran expuestos, permite garantizar la confidencialidad, integridad y disponibilidad de la información a través de la aplicación de opciones apropiadas de tratamiento de riesgos de seguridad de la información y seguridad digital.

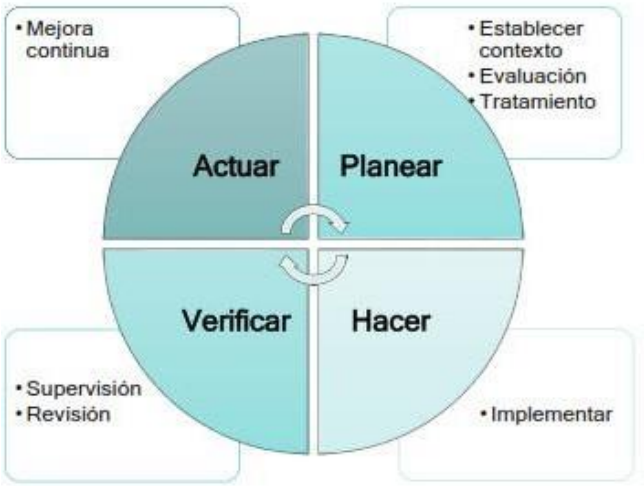
Teniendo en cuenta lo anterior, se actualiza el presente documento dando cumplimiento a lo establecido en el Decreto 612 de 2018, actualizando las acciones para la implementación del plan de seguridad y privacidad de la Información al interior de la Empresa Férrea Regional.

1. Generalidades

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.



2. Alcance

Inicia con la posibilidad de afectación de la confidencialidad/privacidad, integridad y disponibilidad de la información, que a su vez puede impactar el debido cumplimiento de la misión y de los objetivos institucionales y finaliza con el tratamiento correspondiente para su control.

3. Objetivo general

Liderar la formulación de metodologías institucionales para identificar, evaluar y analizar los riesgos de seguridad de la información, mediante una gestión integral y la implementación de controles físicos y digitales previniendo así incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y al alto desempeño a nivel institucional, propendiendo así por el acceso, uso efectivo y apropiación masiva de las TIC, a través de políticas y programas de mitigación del riesgo.

3.1 Objetivos Específicos

- Definir, reformular y formalizar los elementos normativos sobre los temas de protección de la información.
- Gestionar los riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de manera integral.
- Mitigar los incidentes de seguridad y privacidad de la Información, seguridad digital de forma efectiva, eficaz y eficiente.
- Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad, continuidad y no repudio de la información de la Empresa.
- Definir los lineamientos necesarios para el manejo de la información tanto física como digital en el marco de una gestión documental basada en la seguridad y privacidad de la Información.
- Generar conciencia para el cambio organizacional requerido para la apropiación de la seguridad y privacidad de la información como eje transversal para la Empresa.
- Dar cumplimiento a los requisitos legales y normativos en materia de seguridad y privacidad de la información, seguridad digital y protección de la información personal.

4. Normatividad aplicable

Dentro de la normatividad legal aplicable vigente, se encuentra:

- 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 de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas Octubre -2018

5. Desarrollo del Plan

5.1 Identificación y valoración de Riesgos

La técnica para la identificación del riesgo para activos de información nos permite desde un punto de vista orientado al negocio y sistémico en su naturaleza, comprender claramente los riesgos sobre los activos de información a los que puede estar expuesto la Empresa Férrea Regional S.A.S, De este modo, contamos con técnicas tradicionales para identificar los riesgos específicos asociados a los activos y complementar este proceso en la medida de lo posible con la identificación de puntos críticos de fallas, análisis de disponibilidad, de vulnerabilidad y de confiabilidad.

La valoración del riesgo consiste principalmente en el establecimiento de la probabilidad de ocurrencia del riesgo identificado, así mismo su nivel de consecuencia o impacto con el fin de estimar la zona de riesgo o severidad.

Para la realización de esta valoración, se debe analizar y evaluar un aspecto importante y es la probabilidad, la cual se basa en el número de veces que en que se pasa por el punto de riesgo en el periodo de un año, así mismo, se define la zona y porcentajes.

La siguiente tabla es usada para la determinación la probabilidad.

Empresa Férrea Regional S.A.S. - EFR S.A.S
Tabla Niveles de Probabilidad
Vigencia 2021

ítem	Probabilidad Frente al Riesgo	Probabilidad %	Frecuencia de la Actividad (*)
1	Muy Baja	20%	Máximo 2 veces X Año
2	Baja	40%	3 a 24 veces X Año
3	Media	60%	25 a 500 veces X Año
4	Alta	80%	501 a 5000 veces X Año
5	Muy Alta	100%	> 5000 veces X Año

(*) Numero de veces que se ejecuta la actividad que conlleva el riesgo
Fuente: *Ilustración Tabla de Probabilidad. Departamento Administrativo de la Función Pública. 2020*

Otro aspecto importante es el impacto el cual se entiende como las consecuencias que pueden ocasionar a la organización la materialización del riesgo. Se basa en la siguiente tabla, considerando la pérdida reputacional y afectación económica o presupuestal.

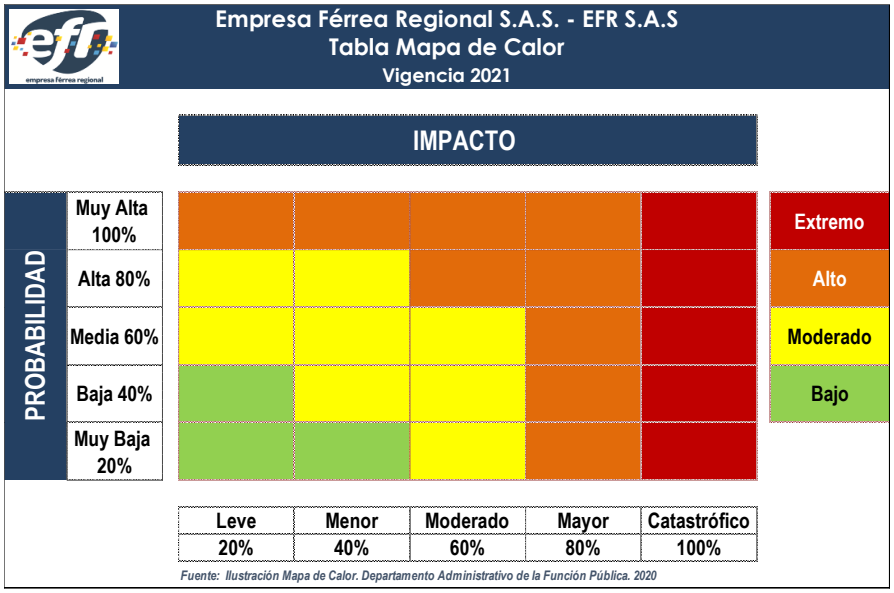
Empresa Férrea Regional S.A.S. - EFR S.A.S
Tabla Niveles de Impacto
Vigencia 2021

ítem	Impacto Frente al Riesgo	Impacto %	Afectación Económica	Pérdida Reputacional (*)
1	Leve	20%	>= 10 SMLMV	El riesgo afecta la imagen de algún área de la Empresa
2	Menor	40%	Entre 11 y 50 SMLMV	El Riesgo afecta la imagen de la Empresa internamente, de conocimieno general nivel interno, de junta directiva, y accionisttas y/o proveedores
3	Moderado	60%	Entre 51 y 100 SMLMV	El riesgo afecta la imagen de la Empresa con algunos usuario de relevancia frente al logro de los objetivos.
4	Mayor	80%	Entre 101 y 500 SMLMV	El riesgo afecta la imagen de la Empresa con efecto publicitario sostenible a nivel de sector adminsitrativo, nivel departamental o municipal
5	Catastrófico	100%	500 SMLMV	El riesgo afecta la imagen de la Empresa a nivel nacional, con efecto publicitario sostenido a nivel país

Nota: *Si en un mismo riesgo estan los 2 impactos (Economico y reputacional) se toma el nivel más alto*

Si se tienen para un mismo riesgo ambos impactos (reputacional y económico) que tienen diferentes niveles se toma el más alto.
Como aspecto final tenemos la evaluación del riesgo el cual permite confrontar los resultados de la calificación del riesgo, con los criterios definidos, de esta forma es posible distinguir la calificación del riesgo.

6. Mapa de Calor



Fuente: Ilustración Mapa de Calor. Departamento Administrativo de la Función Pública. 2020

7. Cronograma

Para dar cumplimiento al ciclo de riesgo, el cronograma se establece anualmente, los riesgos de seguridad digital identificados se reflejarán en el Mapa de Riesgos Institucional, donde se establecerán las acciones de control y las fechas para implementar dichos controles, la oficina de sistemas e informática apoyará el proceso de definición de los controles con los líderes de cada uno de los grupos o dependencias.

HITOS	1	2	3	4	5	6	7	8	9	10	11	12
PROGRAMACIÓN Y AGENDAMIENTO DE ENTREVISTAS												
ENTREVISTA CON LOS LÍDERES DE PROCESO												
IDENTIFICACIÓN Y CALIFICACIÓN DE RIESGOS												
VALORACIÓN DEL RIESGO RESIDUAL												
MAPAS DE CALOR DONDE SE UBICAN LOS RIESGOS												
PLAN DE TRATAMIENTO DE RIESGOS												
SEGUIMIENTO Y CONTROL												

8. Seguimiento

Para garantizar el correcto resultado durante el seguimiento y revisión debe asegurar que las acciones establecidas en los mapas de riesgo se están llevando a cabo y evaluar la eficacia en su implementación, adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden influir en la aplicación de acciones preventivas.