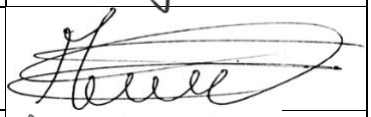
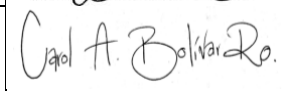
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

EMPRESA FÉRREA REGIONAL S.A.S
EFR.S.A.S

BOGOTÁ, ENERO 2022

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	28/01/2022	Actualización del documento para la vigencia 2022.

RESPONSABLE	CARGO	NOMBRE	FIRMA
APROBÓ	Subgerente General	Oscar Eduardo Rodríguez Lozano	
REVISO	Jefe Oficina de Riesgos y Seguridad	Patricia Gómez Moreno	
ELABORÓ	Jefe Oficina Asesora de Planeación Institucional	Esteban Mancera Orjuela	
	Contratista Dirección Administrativa y Financiera	Carol Andrea Bolívar Rodríguez	
	Contratista Dirección Administrativa y Financiera	Ronal Giovanni Quecan Fetecua	

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.

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.

Formalizar de manera eficaz la seguridad de la información y riesgos de seguridad digitalde 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.

1. Generalidades

La técnica de análisis de riesgo para activos de información nos permite desde un puntode 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 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

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

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 digitaly continuidad de la operación de manera integral.
- ☐ Mitigar los incidentes de seguridad y privacidad de la Información, seguridad digitalde 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

- ☐ Decreto 1078 de 2015 Por medio del cual se expide el Decreto Único Reglamentariodel 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”.

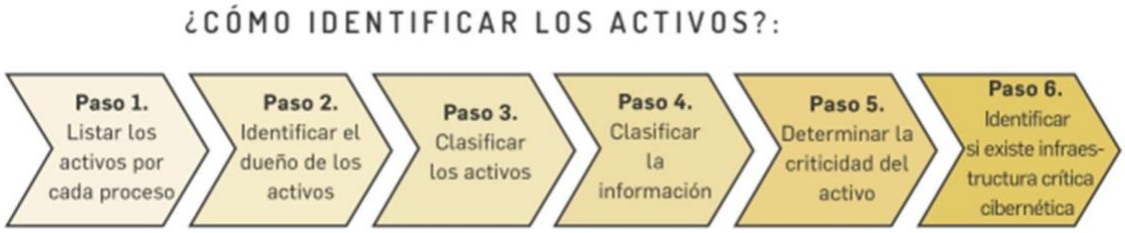
- ☐ Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP 2020

5. Desarrollo del Plan

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 elcontexto 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



5.2 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 expuesta

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 delo 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.

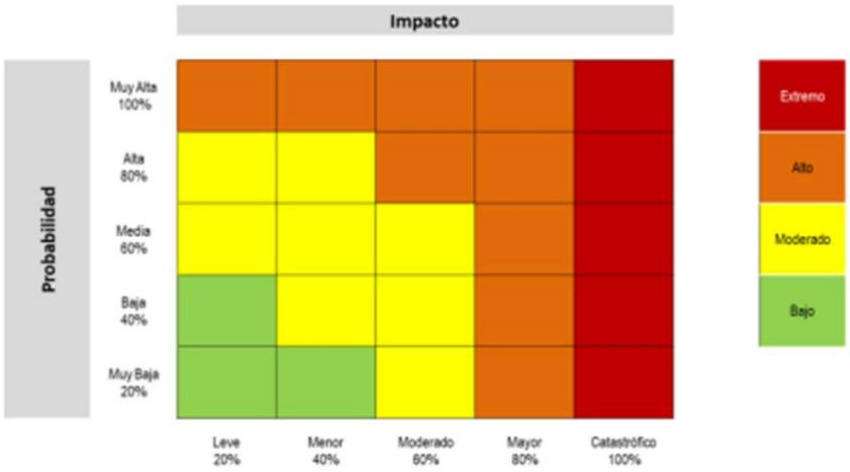
	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad 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%

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.

	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

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



7. 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 2022			
			Trim 1	Trim 2	Trim 3	Trim 4
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 contratadas)	Dirección administrativa y financiera	Inventario de activos de información		X		
Identificación y valoración de riesgos de Seguridad Digital	Dirección administrativa y financiera / Oficina de Planeación	Matriz de riesgos de seguridad digital			X	
Identificación de Controles de Seguridad Informática.	Dirección administrativa y financiera	Controles implementados			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	
Realizar evaluación de vulnerabilidades informáticas	Dirección administrativa y financiera	Informe de vulnerabilidades			X	
Adoptar acciones para tratar los riesgos identificados y fortalecer los controles existentes	Dirección administrativa y financiera / Oficina de Planeación	Seguimiento a acciones para abordar riesgos			X	X