

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: PL-EFR-GFT-003
		VERSIÓN: 06
		FECHA: 30/ENE/2024

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

EMPRESA FÉRREA REGIONAL
S.A.S

BOGOTÁ, ENERO 2024



SC-2000242



CO-SC-2000242

Av. Calle 26 No. 57 - 83 – Oficina P7-T8
Edificio T7-T8 Ciudad Empresarial Sarmiento Angulo
Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (601) 880 7630

 empresaferreregional
  @efrcundinamarca
  @efrcundinamarca
<https://www.efr-cundinamarca.gov.co/>

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: PL-EFR-GFT-003
		VERSIÓN: 06
		FECHA: 30/ENE/2024

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	30/01/2024	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.

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	Ronal Giovanni Quecan Fetecua	Firmado Electrónicamente
	Contratista Oficina de Riesgos y Seguridad	María Alejandra Castiblanco	Firmado Electrónicamente



SC-2000242



CO-SC-2000242

Av. Calle 26 No. 57 - 83 – Oficina P7-T8
Edificio T7-T8 Ciudad Empresarial Sarmiento Angulo
Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (601) 880 7630

empresaferrerearegional
 @efrcundinamarca
 @efrcundinamarca
<https://www.efr-cundinamarca.gov.co/>



PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CÓDIGO: PL-EFR-GFT-003

VERSIÓN: 06

FECHA: 30/ENE/2024

TABLA DE CONTENIDO

INTRODUCCIÓN

3

- 1. 4
 - 1.1. 4
- 2. 4
- 3. 5
- 4. 5
- 5. 6
 - 5.1. 6
 - 5.2. 7
- 6. 9
- 7. 10
- 8. 11



SC-2000242



CO-SC-2000242

Av. Calle 26 No. 57 - 83 – Oficina P7-T8
Edificio T7-T8 Ciudad Empresarial Sarmiento Angulo
Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (601) 880 7630

<https://www.efr-cundinamarca.gov.co/>

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: PL-EFR-GFT-003
		VERSIÓN: 06
		FECHA: 30/ENE/2024

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 eventos que afectan 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.

Este plan busca administrar 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.

1. OBJETIVO GENERAL

Identificar, evaluar y analizar los riesgos de seguridad de la información, mediante una gestión integral y la implementación de controles físicos y digitales que prevengan incidentes y garanticen el acceso, uso efectivo y apropiación masiva de las TIC, a través de políticas y programas de mitigación del riesgo.

1.1. 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.

2. ALCANCE

Inicia el análisis del contexto de la empresa y la posibilidad de afectación a la confidencialidad/privacidad, integridad y disponibilidad de la información, que a su vez puede



Av. Calle 26 No. 57 - 83 – Oficina P7-T8
Edificio T7-T8 Ciudad Empresarial Sarmiento Angulo
Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (601) 880 7630

 empresaferrerearegional
  @efrcundinamarca
  @efrcundinamarca
<https://www.efr-cundinamarca.gov.co/>

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: PL-EFR-GFT-003
		VERSIÓN: 06
		FECHA: 30/ENE/2024

impactar el cumplimiento de la misión y de los objetivos institucionales y finaliza con el tratamiento y mitigación de vulnerabilidades.

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

- **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).
- **CONTROL O MEDIDA:** Medida que permite reducir o mitigar un riesgo.
- **IMPACTO:** consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **PROBABILIDAD:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.



5C-2000242



CO-5C-2000242

Av. Calle 26 No. 57 - 83 – Oficina P7-T8
Edificio T7-T8 Ciudad Empresarial Sarmiento Angulo
Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (601) 880 7630

 empresaferreregional
  @efrcundinamarca
  @efrcundinamarca
<https://www.efr-cundinamarca.gov.co/>

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: PL-EFR-GFT-003
		VERSIÓN: 06
		FECHA: 30/ENE/2024

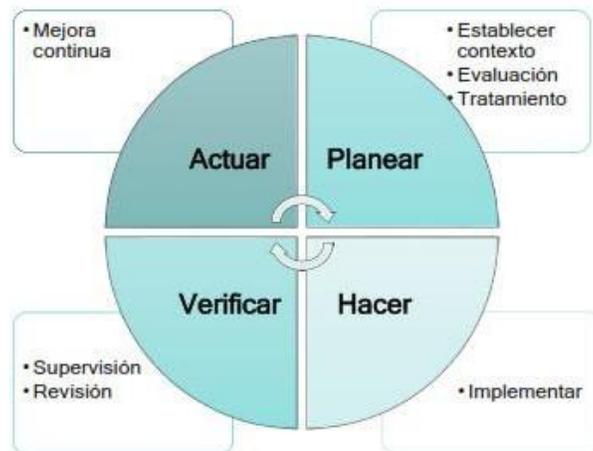
- **RIESGO DE SEGURIDAD DE LA INFORMACIÓN:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **RIESGO:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
- **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 este 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:



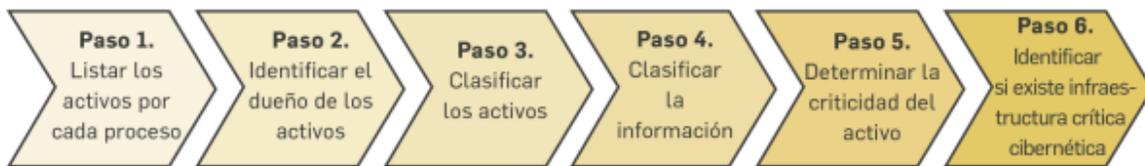
Av. Calle 26 No. 57 - 83 – Oficina P7-T8
Edificio T7-T8 Ciudad Empresarial Sarmiento Angulo
Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (601) 880 7630

 empresaferrerearegional
  @efrcundinamarca
  @efrcundinamarca
<https://www.efr-cundinamarca.gov.co/>

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: PL-EFR-GFT-003
		VERSIÓN: 06
		FECHA: 30/ENE/2024

- 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

¿CÓMO IDENTIFICAR LOS ACTIVOS?:



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 periodo 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



Av. Calle 26 No. 57 - 83 – Oficina P7-T8
Edificio T7-T8 Ciudad Empresarial Sarmiento Angulo
Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (601) 880 7630


<https://www.efr-cundinamarca.gov.co/>

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: PL-EFR-GFT-003
		VERSIÓN: 06
		FECHA: 30/ENE/2024

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 integridad, disponibilidad y confidencialidad 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.



5C-2000242



CO-5C-2000242

Av. Calle 26 No. 57 - 83 – Oficina P7-T8
Edificio T7-T8 Ciudad Empresarial Sarmiento Angulo
Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (601) 880 7630

empresaferrerearegional
 @efrcundinamarca
 @efrcundinamarca
<https://www.efr-cundinamarca.gov.co/>



PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CÓDIGO: PL-EFR-GFT-003

VERSIÓN: 06

FECHA: 30/ENE/2024

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

6. 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.

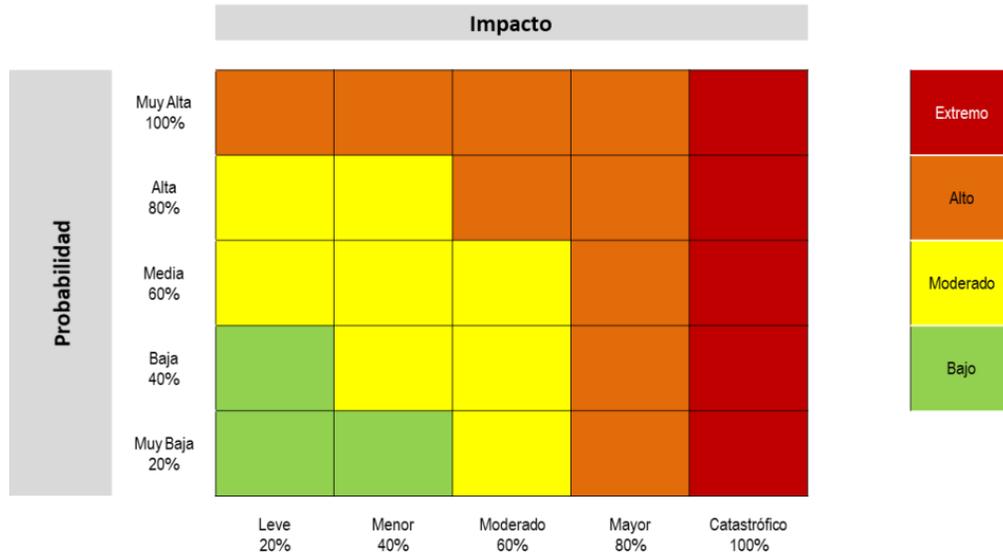


Av. Calle 26 No. 57 - 83 – Oficina P7-T8
Edificio T7-T8 Ciudad Empresarial Sarmiento Angulo
Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (601) 880 7630

<https://www.efr-cundinamarca.gov.co/>

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: PL-EFR-GFT-003
		VERSIÓN: 06
		FECHA: 30/ENE/2024

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

7. 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



SC-2000242



CO-SC-2000242

Av. Calle 26 No. 57 - 83 – Oficina P7-T8
Edificio T7-T8 Ciudad Empresarial Sarmiento Angulo
Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (601) 880 7630

 empresaferreregional
  @efrcundinamarca
  @efrcundinamarca
<https://www.efr-cundinamarca.gov.co/>

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: PL-EFR-GFT-003
		VERSIÓN: 06
		FECHA: 30/ENE/2024

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.

8. 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 2024			
			T ri m 1	T ri m 2	T ri m 3	T ri m 4
Adelantar proceso de asignación de OS para continuidad en la estructuración y aplicación del sistema de gestión de seguridad de la información	Dirección administrativa y financiera / Oficina de Planeación	Asignación recurso humano		X		
Socialización sobre la gestión de riesgos de seguridad digital y sus controles	Dirección administrativa y financiera / Oficina de Planeación / Oficina de riesgos y seguridad	Listados de asistencia		X		
Verificación De La identificación y valoración de riesgos de Seguridad Digital	Dirección administrativa y financiera / Oficina de Planeación / Oficina de riesgos y seguridad	Matriz de riesgos de seguridad digital		X		
Generar la implementación de los controles aprobados de Seguridad Informática.	Dirección administrativa y financiera	Controles implementados			X	



Av. Calle 26 No. 57 - 83 – Oficina P7-T8
Edificio T7-T8 Ciudad Empresarial Sarmiento Angulo
Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (601) 880 7630



PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CÓDIGO: PL-EFR-GFT-003

VERSIÓN: 06

FECHA: 30/ENE/2024

Actividad	Responsable	Entregable / producto	Programación 2024			
			T r i m 1	T r i m 2	T r i m 3	T r i m 4
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 / Oficina de riesgos y seguridad	Seguimiento a acciones para abordar riesgos			X	X



SC-2000242



CO-SC-2000242

Av. Calle 26 No. 57 - 83 – Oficina P7-T8
Edificio T7-T8 Ciudad Empresarial Sarmiento Angulo
Bogotá D.C. – Colombia
Código Postal: 110931 – Teléfono: (601) 880 7630

<https://www.efr-cundinamarca.gov.co/>