SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN SGSPI - MINTIC

Nombre del documento	Plan de tratamiento riesgos SPI.docx
Versión del documento	4.0
Fecha	14/12/2021
Resumen	El presente documento define las medidas de seguridad identificadas para desarrollar e implementar al 31 de diciembre del 2022 el plan de tratamiento para los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones.
Anexo	Declaración de aplicabilidad

Control de Cambios		
Fecha	**Versión**	**Descripción**
31/07/2018	1.0	Creación.
12/12/2019	**2.0**	**Seguimiento.**
15/12/2020	**3.0**	**Actualización.**
14/12/2021	**4.0**	**Actualización.**

	Fecha	Nombre	Cargo o Perfil
Elaboró	14/12/2021	Giovanni A. Espitia Roa	Contratista Equipo Seguridad y Privacidad de la Información
Revisó	15/12/2021	Andrés Díaz Molina	Asesor Despacho de la Ministra – Oficial de Seguridad y Privacidad de la Información
Aprobó	29/12/2021	Comité MIG # 52	

TABLA DE CONTENIDO

1. RESUMEN EJECUTIVO 3
2. INTRODUCCIÓN 4
3. DEFINICIONES 5
4. OBJETIVOS 6
5. ALCANCE 7
6. MARCO REFERENCIAL 8
6.1. POLÍTICA DE ADMINISTRACION DE RIESGOS 8
7. METODOLOGÍA 10
7.1. DESARROLLO METODOLÓGICO 11
7.2. OPORTUNIDAD DE MEJORA 12
8. RECURSOS 13
9. PRESUPUESTO 14
10. MEDICIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 15
10.1 MEDICIÓN 15

1. RESUMEN EJECUTIVO

Mediante la definición del Plan de Tratamiento de Riesgos se busca establecer medidas para mitigar los riesgos presentes en su análisis (perdida de la confidencialidad, perdida de integridad de los activos y perdida de disponibilidad de los activos) evitando situaciones que generen incertidumbre en el cumplimiento de los objetivos del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones

El Plan de Tratamiento de Riesgo se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos identificados en los procesos de la entidad, estas acciones son organizadas en forma de medias de seguridad, y para cada una de ellas se define el nombre de la medida, objetivo, justificación, responsable de la medida y su prioridad, el Ministerio TIC define medidas que serán aplicadas durante la vigencia del plan.

Las anteriores medidas se definieron teniendo en cuenta la información del análisis de riesgos, de las necesidades de los procesos de la entidad en cuanto a la seguridad y privacidad de la información y proporcionó las herramientas necesarias para definir cada una de las características de las medidas y la definición de los pasos a seguir para su ejecución.

2. INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicionalmente busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el Entorno TIC para el Desarrollo Digital, ciudadanos y hogares empoderados del Entorno Digital, Transformación Digital Sectorial y Territorial e Inclusión Social Digital.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3995 de 2020, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001:2013, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital.

3. DEFINICIONES

- **Riesgo:** es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

- **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).

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

- **Probabilidad:** es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

- **Impacto:** son las consecuencias que genera un riesgo una vez se materialice.

- **Control o Medida:** acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

4. OBJETIVOS

- Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios a los que el Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones pueda estar expuesto, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad, privacidad y autenticidad de la información.

- Cumplir con los requisitos legales, reglamentarios, regulatorios y de las normas técnicas colombianas.

- Gestionar riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios, de acuerdo con los contextos establecidos en la Entidad.

- Fortalecer y apropiar conocimiento referente a la gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones.

5. ALCANCE

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios, que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. Junto con Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016)[1]: se dan los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en el Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones

El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos que se encuentren en los niveles Moderado, Alto y Extremo acorde con los lineamientos definidos por el Ministerio, los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad.

[1] Ibídem.

6. MARCO REFERENCIAL

6.1. POLÍTICA DE ADMINISTRACION DE RIESGOS

El Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, a través de su Modelo Integrado de Gestión, se compromete a mantener una cultura de la gestión del riesgo que permita fortalecer las medidas de prevención, monitoreo y seguimiento al control para mitigar la posible ocurrencia de riesgos, en las actividades desarrolladas por la Entidad asociadas con la responsabilidad de diseñar, adoptar y promover las políticas**,** planes, programas, iniciativas y proyectos del sector TIC, mediante mecanismos, sistemas y controles que detecten hechos asociados, de manera Integral, con la estrategia, la corrupción, seguridad y privacidad de la información, seguridad digital y continuidad de la operación, aspectos ambientales y de seguridad y salud en el trabajo, que puedan afectar el cumplimento de los objetivos institucionales, el aprovechamiento al máximo los recursos destinados y la atención a nuestros grupos de interés

.

El objetivo de la política es establecer los parámetros necesarios para una adecuada gestión de los riesgos de gestión, corrupción, Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo único de Tecnologías de la Información y las comunicaciones procurando que no se materialicen, atendiendo los lineamientos establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP, orientando a la toma de decisiones oportunas y minimizando efectos adversos al interior de la Entidad, con el fin de dar continuidad a la gestión institucional y asegurar el cumplimiento de los compromisos con los Grupos de interés.

El tratamiento de riesgos es la respuesta establecida por la primera línea de defensa, es decir, el líder o responsable del proceso junto con su equipo de trabajo para la mitigación de los diferentes riesgos.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

Aceptar el riesgo: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción es aceptado). La aceptación del riesgo puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y, por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

Reducir el riesgo: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. Deben seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

Evitar el riesgo: Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

Compartir el riesgo: Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad. Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización.

La gestión de riesgos de Seguridad y privacidad de la Información, seguridad digital y continuidad de la operación de los servicios le permite al Ministerio realizar una identificación, análisis y tratamiento de los riesgos que puedan generar

afectación al cumplimiento de los objetivos de sus procesos, contribuyendo en la toma de decisiones, y en la prevención de la materialización de estos. La administración de riesgos de seguridad y privacidad de la información se encuentra enfocada en identificar, analizar, valorar y tratar las amenazas y vulnerabilidades de los activos de información de la entidad, teniendo presente su criticidad y protección. Las etapas presentes en la gestión de riesgos permiten alinearlas con los objetivos, estrategias y políticas corporativas, logrando un nivel de riesgo que pueda aceptar o asumir la Alta Dirección.

7. METODOLOGÍA

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos identificados en la entidad, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016)[2]:

Gestión	Actividades	Tareas	Responsable de la Tarea	Fecha Inicio	Fecha Final
Gestión de Riesgos	Actualización de lineamientos de riesgos	Apoyar cuando se requiera la actualización de la política, metodología y lineamientos de la gestión de riesgos	Equipo de Gestión de Riesgos	1-feb-22	30-nov-22
	Sensibilización	Socialización de lineamientos y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Equipo de Gestión de Riesgos	1-mar-22	31-may-22
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Contexto, Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Equipo de Gestión de Riesgos	1-mar-22	31-may-22
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Equipo de Gestión de Riesgos	1-mar-22	31-may-22
	Aceptación de Riesgos Identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento	Equipo de Gestión de Riesgos	2-may-22	15-jun-22
	Publicación	Publicación mapas de riesgos de los procesos en SIMIG	Equipo de Gestión de Riesgos	1-jun-22	30-jun-22
	Seguimiento Fase de Tratamiento	Seguimiento controles y planes de tratamiento de riesgos los identificados (verificación de evidencias)	Equipo de Gestión de Riesgos	17-ene-22	23-dic-22
	Seguimiento valoración de riesgos residuales	Seguimiento a la valoración de los riesgos residuales	Equipo de Gestión de Riesgos	17-ene-22	23-dic-22
	Mejoramiento	Identificación de oportunidades de mejora acorde al seguimiento de los planes de tratamiento y al seguimiento de la valoración de los riesgos residuales	Equipo de Gestión de Riesgos	17-ene-22	23-dic-22
		Revisión y/o actualización de lineamientos de Riesgos de Seguridad y privacidad de la información de acuerdo con las observaciones presentadas.	Equipo de Gestión de Riesgos	1-jul-22	23-dic-22
	Monitoreo y Revisión	Medición, presentación y reporte de indicadores	Equipo de Gestión de Riesgos	17-ene-22	30-dic-22

Los controles seleccionados serán confrontados con los estándares ISO 27001:2013 y su anexo A; a fin de determinar las falencias del Ministerio en este sentido.

[2] Ibidem.

7.1. Desarrollo metodológico

Establecimiento del contexto

El contexto en términos generales relaciona los aspectos externos, internos y del proceso que se deben tener en cuenta para gestionar los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones. A partir del contexto es posible establecer las posibles causas de los riesgos a identificar. De esta forma para la definición del contexto se seguirán las metodologías dispuestas en la entidad para lograr establecer las posibles causas y determinar la identificación de los riesgos.

Identificación del riesgo

Para la identificación de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones se debe tener en cuenta diferentes aspectos como infraestructura física, áreas de trabajo, entorno y ambiente en general, para lo cual se hace indispensable que cada uno de los procesos tenga identificado los activos de información, y reconocer las situaciones potenciales que causarían daño a la entidad poniendo en riesgo el logro de los objetivos establecidos.
La falta de apropiación en temas referentes a la seguridad de la información o la ausencia de controles (vulnerabilidades) puede ser aprovechadas por una amenaza causando la materialización de un riesgo (Incidente), por lo que es preciso identificar: El atributo de la triada de la información afectado (Confidencialidad, Integridad, Disponibilidad), el proceso dueño del riesgo, activo de información afectado, amenazas, vulnerabilidades y consecuencias.
Para la identificación se pueden abarcar datos históricos, análisis teóricos, opiniones informadas y expertas, y las necesidades de las partes involucradas.

Valoración del riesgo

La valoración de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones se realizará acorde a la metodología para la administración de riesgos mencionada en la Guía para la administración del riesgo y el diseño de controles en entidades públicas emitida por el Departamento Administrativo de la Función Pública y adoptada por el Ministerio para la gestión del riesgo y las tablas de impacto definidas para el Ministerio.
Es así como en mesas de trabajo con los procesos se analiza el contexto, se identifican los riesgos y se realiza el análisis de la probabilidad e impacto como valoración preliminar para identificar el nivel del riesgo inherente, asociando sus vulnerabilidades e identificando los controles para mitigarlas. A estos controles se le identifican las variables a evaluar para el adecuado diseño de controles como son: responsable, periodicidad, propósito, cómo se realiza la actividad de control, observaciones o desviaciones y la evidencia de la ejecución del control. Adicionalmente se evalúa que cada control se ejecute de manera consistente, de tal forma que pueda mitigar el riesgo. Esta valoración se realiza de acuerdo con las tablas y metodología establecida y mencionada en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP

Definición y aprobación de mapas de riesgos y planes de tratamiento.

Una vez concluidas las etapas de la administración de riesgos y se obtenga la valoración de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios del Ministerio, los líderes de los procesos deberán emitir un memorando de la aprobación de los mapas de riesgos. De igual forma en este memorando aprobarán los planes de tratamiento con las actividades requeridas que permitan mitigar aquellos riesgos cuyo nivel residual este en zona Moderada, Alta o Extrema.

Materialización

En el caso de materializarse un riesgo, este debe ser reportado de acuerdo con el procedimiento de gestión de incidentes de seguridad y privacidad de la información. Así mismo se deberá analizar el riesgo y validar en qué nivel queda posterior a la materialización, registrando los cambios respectivos en el mapa de riesgos. En caso de que se materialice un riesgo que no esté identificado, deberá ser reportado para que se inicie su correspondiente identificación en la matriz.

7.2. Oportunidad de Mejora

El Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones no sólo deberá centrarse en los riesgos identificados, sino que este análisis o apreciación del riesgo debe ser la base para identificar oportunidades. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

8. RECURSOS

El Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, en el marco de la gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios, dispone de los siguientes recursos.

RECURSOS	VARIABLE
Humanos	La Oficina de Tecnologías de la información a través del proceso de seguridad y privacidad de la información es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua.
Técnicos	Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital Herramienta para la gestión de riesgos (Matriz de Riesgos SGSI)
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías

9. PRESUPUESTO

La estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios identificados en la entidad, corresponderá al dueño del riesgo (líder del proceso), quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos y del plan de tratamiento.

10. MEDICIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El monitoreo y seguimiento de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios del Ministerio aprobados por los procesos, así como de sus controles y planes de tratamiento, se realiza por parte del equipo de Seguridad y Privacidad de la Información teniendo en cuenta la periodicidad y fechas de cumplimiento establecidas, validando los resultados de los seguimientos realizados así como el cargue de los soportes correspondientes a los controles definidos.
Una vez los procesos realicen el reporte de cumplimiento de sus planes de tratamiento y controles, los profesionales del proceso de Seguridad y Privacidad de la Información realizan la revisión y validación de esta información, con el fin de reportar la medición de la gestión del riesgo a través del indicador que tiene como propósito medir el nivel de implementación de los controles de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones

10.1 MEDICIÓN

La medición se realiza con un indicador que está orientado principalmente a determinar el porcentaje de ejecución de los controles definidos para mitigar los riesgos identificados en los sistemas de gestión de la entidad.

HOJA DE VIDA DEL INDICADOR

1. **Nombre del indicador:** Controles del Sistema Integrado de Gestión gestionados

2. **¿ Cual es el objeto del indicador?**
Identificar el porcentaje de los controles ejecutados del Sistema Integrado de Gestión El control es la medida que modifica el riesgo (procesos, políticas,

3. **¿ Cual es la definición del indicador?**
Controles por cada uno de los sistemas de gestión (SGC, SGSPI, SGSST, SGA)
SGC: Sistema de Gestión de Calidad
SGSPI: Sistema de Gestión de Seguridad y Privacidad de la Información
SGSST: Sistema de Gestión de Seguridad y Salud en el Trabajo
SGA: Sistema de Gestión Ambiental

4. **¿ Cual es la fórmula de cálculo del indicador?**
(Promedio de controles gestionados del SGC + Promedio de controles gestionados del SGSPI + Promedio de controles gestionados del SGSST + Promedio de controles gestionados del SGA)/4

5. **¿Cuáles son las variables para el cálculo del indicador?.** Relacione para cada variable la fuente de datos y la entidad responsable

	Variables	Fuente de datos para la variable (operación estadística o registro administrativo)	Entidad responsable
a.	Promedio de Controles gestionados del SGC	Mapa de Riesgos	MinTIC
b.	Promedio de Controles gestionados del SGSPI	Mapa de Riesgos	MinTIC
c.	Promedio de Controles gestionados del SGSST	Matriz de identificación de peligro y valoración de riesgo ocupacionales	MinTIC
d.	Promedio de Controles gestionados del SGA	Matriz de aspectos e impactos	MinTIC

6. **¿Cuál es la unidad de medida del indicador?**
Porcentaje

7. **¿Cuál es la tendencia del indicador?**
Positiva

8. **¿Cuál es el tipo de indicador?**
Eficacia ■ Eficiencia □

9 **Parametrización del indicador**

Metas:		
Rango		Calificación
Desde	Hasta	
81%	100%	Alto
61%	80,0%	Medio
0%	60,0%	Bajo