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

Versión 6

Ministerio de Tecnologías de la Información y las Comunicaciones

Despacho del Ministro
GIT de Seguridad y Privacidad de la Información

ECOSISTEMA SEGURO

TABLA DE CONTENIDO

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 confidencialidad, perdida de integridad y perdida de disponibilidad de los activos de información), lo que permite evitar 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 actividades, definiendo para cada una de ellas las tareas, el responsable y sus fechas de ejecución que serán aplicadas durante la vigencia del plan.

Las actividades se definieron teniendo en cuenta la información del análisis de riesgos, de las necesidades y el contexto de los procesos de la entidad en cuanto a seguridad y privacidad de la información proporcionando las herramientas necesarias para identificar sus características y definir 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 (riesgos de interrupción) 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 del proceso, 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 seguimiento a lo recomendado por el Documento CONPES 3995 de 2020 y el Decreto Único Reglamentario del Sector TIC, Decreto 1078 de 2015, que señala la el habilitador de seguridad y privacidad de la Información, reglamentado por la Resolución 500 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad, acogiendo las buenas prácticas y los lineamientos de los estándares ISO 27001, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas establecidos en el Modelo Integrado de Planeación y Gestión.

Teniendo en cuenta lo anterior, se actualiza el presente documento dando cumplimiento a lo establecido en el Decreto 612 de 2018, actualizando el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información al interior del Ministerio de Tecnologías de la Información y las Comunicaciones, aprobado mediante acta de la sesión # 77 de comité del Modelo Integrado de Gestión – MIG del 28 de diciembre de 2023.

3. DEFINICIONES[1]

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

- **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).

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

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

- **Control o Medida:** Medida que permite reducir o mitigar un riesgo.

[1] Tomado de Guía para la administración del riesgo y el diseño de controles en entidades públicas - DAFP

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 (riesgos de interrupción) 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 en materia de seguridad y privacidad de la información, seguridad digital y protección de la información personal.

- Gestionar los riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción), de acuerdo con los contextos establecidos en los procesos de 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 (riesgos de interrupción) 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 (riesgos de interrupción), 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. Adicionalmente dar 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 todos los riesgos en especial los que se encuentren en los niveles Moderado, Alto y Extremo acorde con los lineamientos definidos por el Ministerio de TIC, teniendo en cuenta que los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad.

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, ejecutar 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 gestión la transparencia y la ética, seguridad y privacidad de la información, seguridad digital y continuidad de la operación, riesgo fiscal, 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[2].

El objetivo de la política es establecer los parámetros necesarios para una adecuada gestión de los Riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de los servicios (riesgos de interrupción) 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.

[2] MIG-TIC-MA-008 lineamientos para la administración de riesgos

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 (riesgos de interrupción) le permite al Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones 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, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) 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)[3]:

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
Gestión de Riesgos	Sensibilización	Socialización de lineamientos y herramienta para la Gestión de Riesgos de Seguridad y privacidad de la Información y Seguridad Digital	Equipo de Gestión de Riesgos	1-mar-24	31-may-24
	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 y Seguridad Digital	Equipo de Gestión de Riesgos	1-mar-24	26-jul-24
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Equipo de Gestión de Riesgos	1-mar-24	26-jul-24
	Aceptación de Riesgos Identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento	Equipo de Gestión de Riesgos	6-may-24	19-jul-24
	Publicación	Publicación mapas de riesgos de los procesos en SIMIG	Equipo de Gestión de Riesgos	3-jun-24	31-jul-24
	Seguimiento Fase de Tratamiento	Seguimiento implementación de controles y planes de tratamiento de riesgos los identificados (verificación de evidencias)	Equipo de Gestión de Riesgos	15-ene-24	27-dic-24
	Mejoramiento	Identificación de oportunidades de mejora acorde al seguimiento de la ejecución de los controles y de los planes de tratamiento	Equipo de Gestión de Riesgos	15-ene-24	27-dic-24
		Revisión y/o actualización de lineamientos de Riesgos de Seguridad y privacidad de la información de acuerdo con las observaciones identificadas.	Equipo de Gestión de Riesgos	1-feb-24	27-dic-24
	Monitoreo y Revisión	Medición, presentación y reporte de indicadores	Equipo de Gestión de Riesgos	15-ene-24	27-dic-24

Los controles seleccionados para mitigar los riesgos de Seguridad y Privacidad de la Información serán confrontados con los estándares ISO 27001; a fin de determinar las falencias del Ministerio en este sentido.

[3] Ibidem.

7.1. Desarrollo metodológico [4]

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 la Operación de los Servicios (riesgos de interrupción) 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 la Operación de los Servicios (riesgos de interrupción) 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

[4] MIG-TIC-MA-008 Lineamientos para la administración de riesgos – sección 10.3 Administración de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios.

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 en el formato del mapa de riesgos: El atributo de la triada de la información afectado (Confidencialidad, Integridad, Disponibilidad), dueño del riesgo (líder del proceso), activo de información afectado, amenazas, vulnerabilidades y consecuencias.
Para determinar los activos afectados es necesario validarlos dentro del inventario de activos de información del proceso en donde en su valoración se estableció la criticidad, la clasificación de la información y otros atributos importantes a tener en cuenta en el análisis del posible riesgo. Es importante mencionar que la identificación de los activos de información se realizó de acuerdo con los lineamientos establecidos por la entidad en los documentos GDO-TIC-MA-014 manual de activos de información y el GDO-TIC-PR-019 Procedimiento Activos de Información.
Por otra parte, la identificación de las posibles amenazas y vulnerabilidades es apoyada por el catálogo definido en el anexo 4 “Lineamientos para la gestión del riesgo en entidades públicas” las cuales son analizadas, validadas y complementadas en las mesas de trabajo con los diferentes procesos, y de acuerdo con éstas se establecen las posibles consecuencias.

Valoración del riesgo

La valoración de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios (riesgos de interrupción) 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 amenazas, vulnerabilidades y consecuencias e identificando los controles asociados al anexo A de la Norma ISO 27001 para mitigarlas. A estos controles se le identifican las variables a evaluar para su adecuado diseño como son: la asignación de un responsable, segregación y autoridad del responsable, tipo de control (preventivo, detectivo o correctivo), implementación (manual o automático), periodicidad, propósito, cómo se realiza la actividad de control, qué pasa con las 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.

Para los riesgos de interrupción, se indica que los controles identificados pueden ser transversales, partiendo del criterio denominado custodio del activo, puesto que cuando dicho custodio es un proceso diferente al proceso que identifica el riesgo o es un tercero, estos controles y planes de tratamiento deben establecerse de manera conjunta. El proceso donde se identifica el riesgo aporta los niveles de probabilidad, impacto y riesgo inherente que genera la posible indisponibilidad del activo

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 la Operación de los Servicios (riesgos de interrupción) del Ministerio, los líderes de los procesos apoyados por los gestores, deberán realizar a través de la plataforma de formalización de documentación definida por el Ministerio, el proceso de aprobación de los mapas de riesgos y de 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 el mapa de riesgos.

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 (riesgos de interrupción), dispone de los siguientes recursos.

<table>
<tr><th>RECURSOS</th><th>VARIABLE</th></tr>
<tr><td>Humanos</td><td>

El Grupo Interno de Trabajo de Seguridad y Privacidad de la Información
Profesional de riesgos del Grupo Interno de Trabajo de Transformación Organizacional
Líderes y gestores de procesos
Dimensión de Seguridad informática de la Oficina de TI
Grupo Interno de Trabajo de Respuesta a Emergencias Cibernéticas de Colombia - COLCERT
Equipo de Trabajo de Seguridad y Privacidad de la Información de la Dirección de Gobierno Digital.

</td></tr>
<tr><td>Técnicos</td><td>Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital del DAFP
Herramienta para la gestión de riesgos (Matriz de Riesgos SGSPI)</td></tr>
<tr><td>Logísticos</td><td>Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.</td></tr>
<tr><td>Financieros</td><td>Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías en el GIT de Seguridad y Privacidad de la Información
<table>
<tr><th>Iniciativa</th><th>Proyecto</th><th>Presupuesto</th></tr>
<tr><td>Fortalecimiento de las capacidades institucionales para la seguridad y Privacidad de la Información</td><td>P1 - Fortalecimiento del Modelo de gestión de seguridad y privacidad de la información.</td><td>$ 156.670.000.oo</td></tr>
</table>
</td></tr>
</table>

9. PRESUPUESTO PARA LA IMPLEMENTACIÓN DE CONTROLES

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 (riesgos de interrupción) 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

El monitoreo y seguimiento de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los Servicios (riesgos de interrupción) del Ministerio aprobados por los procesos, así como de sus controles y planes de tratamiento, se realiza por parte del Grupo Interno de Trabajo 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 la operación de los Servicios (riesgos de interrupción) del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones

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.

1.	**Nombre del indicador:**	Controles del Sistema Integrado de Gestión gestionados
2.	**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, dispositivos, prácticas u otras acciones), y se ejecuta según su periodicidad establecida en el mapa de riesgos a través del cumplimiento de cada una de las evidencias que ayudan a mitigar los riesgos de los procesos.
3.	**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	**Fórmula de cálculo del**	(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. **Identifique las variables para el cálculo del indicador.**

	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	MinTIC
d.	Promedio de Controles gestionados del SGA	Matriz de aspectos e impactos ambientales	MinTIC

6.	**Unidad de medida del Indicad**	Porcentaje
7.	**Tendecnia del Indicador.**	Positiva
8.	**Tipo de Indicador.**	Eficacia ■ Eficiencia ▯ Efectividad ▭

9. **Parametrización del indicador.**

Metas:		
Rango		Calificación
Desde	Hasta	
90%	100%	Alto
70%	89,9%	Medio
0%	69,9%	Bajo

11. 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.
26/12/2022	5.0	Actualización del documento por cambio de vigencia.
28/12/2023	6.0	Actualización del documento por cambio de vigencia.