



Plan de Tratamiento de Riesgos de Seguridad de la Información - GTIC 2024

CONTENIDO

1.	INTRODUCCIÓN	3
2.	GENERALIDADES.....	3
3.	MARCO NORMATIVO	3
4.	ALINEACIÓN INSTITUCIONAL.....	5
5.	OBJETIVO GENERAL	6
6.	OBJETIVOS ESPECÍFICOS	6
7.	ALCANCE	6
8.	DETALLE DEL PLAN.....	7
9.	CRONOGRAMA.....	7
10.	GLOSARIO.....	8
11.	RESPONSABLE DEL PLAN	9

1. INTRODUCCIÓN

Las decisiones relacionadas con los riesgos se deben basar en los criterios de aceptación institucionales y las opciones de tratamiento del riesgo, y en el enfoque de gestión que la Entidad ha adoptado. En ese sentido, el plan de tratamiento de riesgos de seguridad de la información debe estar alineado con las necesidades de protección requeridas por cada uno de los procesos institucionales y debe estar acorde con los resultados de valoración de los riesgos, la efectividad de los controles dispuestos y el valor residual del riesgo una vez se hayan aplicado los controles disponibles.

Aunado a la aceptación del riesgo residual por parte de cada uno de los líderes de los procesos institucionales, y acorde con lo dispuesto por la metodología de gestión de riesgos adoptada por el Ministerio, se disponen de actividades específicas para tratamiento, en caso de ser requeridas según esta metodología, o cuando el líder del proceso disponga la necesidad de hacer un seguimiento especial a ciertos riesgos que puedan comprometer la seguridad de la información a su cargo.

2. GENERALIDADES

El Ministerio de Transporte, realiza la gestión integral de riesgos que incluye las etapas de identificación, valoración inherente, identificación y valoración de controles, el cálculo del valor residual y la determinación de políticas de tratamiento de riesgos. Esta gestión involucra a los riesgos de seguridad de la información.

El plan de tratamiento de riesgos de seguridad de la información es un instrumento que brinda a la Entidad un medio orientador para la adecuada gestión de aquellos riesgos que por su impacto en la gestión ministerial o en el propósito de sus procesos puede afectar la operación normal de ellos, razón por la cual además de identificarlos, realiza una gestión detallada de seguimiento de las acciones adoptadas como política de tratamiento y así dar un parte de tranquilidad, pues permite prepararse ante una eventual materialización de estos riesgos, cuyo valor residual es mayor al nivel deseado por la Alta Dirección.

3. MARCO NORMATIVO

- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Ley 2108 de 2021. Ley de Internet como servicio público esencial y universal, o por medio de la cual se modifica la Ley 1341 de 2009 y se dictan otras disposiciones.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014. Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.

- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- 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 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- Decreto 1083 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.
- Decreto 728 de 2017. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
- Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- Decreto 2106 de 2019. Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública
- Decreto 620 de 2020. Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 Y 64 de la Ley 1437 de 2011, los literales e, j y literal a del párrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- Decreto 088 de 2022. Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea.
- Decreto 338 de 2022. Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 de Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.
- Decreto 767 de 2022. 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.
- Decreto 1389 de 2022. Por el cual se adiciona el Título 24 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para la gobernanza en la infraestructura de datos, y se crea el Modelo de gobernanza de la infraestructura de datos.
- Directiva Presidencial 03 de 2021. Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
- Directiva Presidencial 02 de 2022. Reiteración de la política pública en materia de seguridad digital.

- CONPES 3854 de 2016. Política Nacional de Seguridad digital.
- Resolución 1519 de 2020, Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
- Resolución MinTIC 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 como habilitador de la política de Gobierno Digital.
- Resolución MinTIC 460 de 2022. Por el cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación.
- Resolución MinTIC 746 de 2022 Por el cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021.
- Resolución MinTIC 1117 de 2022. Por la cual se establecen los lineamientos de transformación digital para las estrategias de ciudades y territorios inteligentes de las entidades territoriales, en el marco de la Política de Gobierno Digital.
- Resolución MinTIC 1951 de 2022. Por la cual se establecen los requisitos, las condiciones y el trámite de la habilitación de los prestadores de servicios ciudadanos digitales especiales; se dan los lineamientos y estándares para la integración de estos servicios y la coordinación de los prestadores con la Agencia Nacional Digital.
- Resolución MinTIC 1978 de 2023. Por la cual se adopta la Versión 3 del Marco de Referencia de Arquitectura Empresarial para el Estado Colombiano como el instrumento para implementar el habilitador de arquitectura de la Política de Gobierno Digital y se dictan otras disposiciones.
- Política Institucional Código: ASG-F-023 - POLITICA DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD DEL MINISTERIO DE TRANSPORTE

4. ALINEACIÓN INSTITUCIONAL

A continuación, se relacionan los componentes que facilitan la alineación del Plan de Tratamiento de riesgos con el Modelo Integrado de Planeación y Gestión MIPG, la Política de gestión y desempeño, así como con los otros Planes, Programas o Proyectos institucionales que se encuentran vigentes:

DIMENSIÓN MIPG POLÍTICA DE GESTIÓN Y DESEMPEÑO PLANES/ PROGRAMAS O PROYECTOS	DESCRIPCIÓN DE RELACIÓN
MIPG. De la Ventanilla hacia adentro. Seguridad Digital.	La seguridad digital requiere que la gestión de riesgos sea ejercida en toda la Entidad, para que se identifiquen de manera anticipada los escenarios que pueden afectar negativamente la operación. De esa forma el Plan de Tratamiento de Riesgos de Seguridad de la Información entrega visibilidad a la Entidad para desplegar acciones preventivas.
Política de Seguridad de la Información.	La intención manifiesta de proteger la confidencialidad, integridad y disponibilidad de la información institucional se basa en una adecuada gestión de los riesgos y del despliegue de acciones de tratamiento para prevenir y controlar aquellos

	eventos que puedan afectar el desempeño o el cumplimiento de los objetivos del Ministerio.
PEI 2024.	En relación con el PEI del cuatrienio 2022-2026, se articula con las líneas estratégicas: 3. Movilidad segura, sostenible e inteligente. Sistemas intermodales de transporte de pasajeros y de carga accesibles, asequibles, seguros, eficientes, sostenibles y con servicios de excelente calidad. Mejoramiento de la calidad y seguridad del servicio de los sistemas de transporte público con enfoque diferencial; y 5. Instituciones fortalecidas, confiables e incluyentes. Fortalecimiento institucional como motor de cambio para recuperar la confianza de la ciudadanía y para el fortalecimiento del vínculo Estado-Ciudadanía; priorizando las Tecnologías de la Información y las Comunicaciones (TIC), la tecnología como factor clave para el cumplimiento de la misión de las entidades del sector.

5. OBJETIVO GENERAL

Establecer el Plan de Tratamiento de los Riesgos de Seguridad y Privacidad de la Información para el Ministerio de Transporte de acuerdo con los resultados obtenidos en la valoración de riesgos y planes de acción definidos por los líderes de proceso para su tratamiento.

6. OBJETIVOS ESPECÍFICOS

A partir de la ejecución del Plan se cumplirán los siguientes objetivos específicos frente al tratamiento de riesgos de seguridad de la información y en general sobre los riesgos de la Entidad.

- Actualizar el estado general de riesgos del Ministerio permitiendo la identificación de aquellos que pueden generar impactos negativos en caso de que se materialicen.
- Validar la efectividad de los planes particulares de tratamiento de riesgos.

7. ALCANCE

El presente plan contempla todos los procesos del Ministerio (Misionales, Estratégicos, Apoyo y de Evaluación), acorde al alcance definido en el Modelo de Seguridad y Privacidad de la Información (MSPI) que se ha definido y adoptado en la Entidad.

8. DETALLE DEL PLAN

La presente versión del Plan de Tratamiento de Riesgos de Seguridad de la Información, pretende ser un instrumento dinámico para la prevención y oportuna intervención en caso de la materialización de riesgos al Interior del Ministerio que puedan llegar a afectar de forma negativa la operación de alguno de sus procesos o que pongan en riesgo los pilares de la seguridad de la información gestionada por cada uno de ellos. Por esta razón se formulan nueve (9), actividades específicas en procura de alcanzar los objetivos propuestos. Estas actividades corresponden a:

- Revisar la política y metodología institucional de riesgos.
- Realizar reuniones de entendimiento con OAP sobre metodología de riesgos.
- Identificar los enlaces SGI por proceso.
- Acompañar la actualización de riesgos por proceso.
- Validar la matriz institucional de riesgos consolidada.
- Identificar los riesgos que ameritan actividades de tratamiento y responsables.
- Monitorear los eventos de materialización de riesgos.
- Apoyar la evaluación de eficiencia de las actividades de tratamiento.
- Validar los resultados de seguimiento periódico a las actividades de tratamiento de riesgos.

9. CRONOGRAMA

Según lo enunciado en el numeral anterior, a continuación, se muestra la propuesta de ejecución del Plan de Tratamiento de Riesgos de Seguridad de la Información para la vigencia 2024.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN					
OBJETIVOS	PRODUCTOS	ACTIVIDADES	RESPONSABLE	VIGENCIA 2024	
				Inicio dd/mm/aaaa	Fin dd/mm/aaaa
Actualizar el estado general de riesgos del Ministerio permitiendo la identificación de aquellos que pueden generar impactos negativos en caso de que se materialicen.	Matriz de riesgos institucional revisada por proceso	Revisar la política y metodología institucional de riesgos.	GTIC - Equipo de Seguridad de la Información	5/02/2024	16/02/2024
		Realizar reuniones de entendimiento con OAP sobre metodología de riesgos.	GTIC - Equipo de Seguridad de la Información - OAP Equipo SGI	19/02/2024	15/03/2024
		Identificar los enlaces SGI por proceso.	GTIC - Equipo de Seguridad de la Información - OAP Equipo SGI	4/03/2024	8/03/2024
		Acompañar la actualización de riesgos por proceso.	GTIC - Equipo de Seguridad de la Información - OAP Equipo SGI	4/03/2024	26/04/2024

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN					
OBJETIVOS	PRODUCTOS	ACTIVIDADES	RESPONSABLE	VIGENCIA 2024	
				Inicio dd/mm/aaaa	Fin dd/mm/aaaa
		Validar la matriz institucional de riesgos consolidada.	GTIC - Equipo de Seguridad de la Información - OAP Equipo SGI	26/04/2024	30/04/2024
	Relación de riesgos potencialmente materializables	Identificar los riesgos que ameritan actividades de tratamiento y responsables.	GTIC - Equipo de Seguridad de la Información - OAP Equipo SGI	29/04/2024	10/05/2024
		Monitorear los eventos de materialización de riesgos.	GTIC - Equipo de Seguridad de la Información	14/05/2024	20/12/2024
Validar la efectividad de los planes particulares de tratamiento de riesgos	Acta de reunión sobre tratamiento de riesgos	Apoyar la evaluación de eficiencia de las actividades de tratamiento.	GTIC - Equipo de Seguridad de la Información - OAP Equipo SGI	14/05/2024	20/12/2024
	Reporte de revisión	Validar los resultados de seguimiento periódico a las actividades de tratamiento de riesgos.	GTIC - Equipo de Seguridad de la Información - OAP Equipo SGI	14/05/2024	20/12/2024

10. GLOSARIO

- Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- Integridad: Propiedad de la información relativa a su exactitud y completitud.
- MSPI: Modelo de Seguridad y Privacidad de la Información.
- PEI: Plan Estratégico Institucional.
- 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.
- Seguridad de la Información: Conjunto de técnicas y métodos encaminados a la preservación de la confidencialidad, integridad y disponibilidad de la información en cualquiera de sus estados, medios de almacenamiento y/o difusión.
- Tratamiento del Riesgo: Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos. El tratamiento de los riesgos puede hacerse mediante la aplicación de la política de tratamiento definida que puede: aceptar el riesgo, reducir el riesgo, evitar el riesgo o compartir el riesgo.
- Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

11. RESPONSABLE DEL PLAN

Responsable Ejecutivo:

Nombre completo: Gustavo Adolfo Vélez Achury

Cargo: Coordinador Grupo TIC

Dependencia: Grupo de Tecnologías de la Información y las Comunicaciones

E mail: gvelez@mintransporte.gov.co

Responsables Operativos:

Nombre completo: Hugo Fernando Ramírez Ospina

Cargo: Contratista Grupo TIC – Oficial de Seguridad de la Información

Dependencia: Grupo de Tecnologías de la Información y las Comunicaciones

E mail: hframirez@mintransporte.gov.co

Nombre completo: Andrés Roberto González González

Cargo: Contratista Grupo TIC – Analista de Seguridad de la Información

Dependencia: Grupo de Tecnologías de la Información y las Comunicaciones

E mail: argonzalez@mintransporte.gov.co