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

2024

PRESENTACIÓN

La Superintendencia de Transporte en su compromiso de propender condiciones de uso confiable en el entorno digital y físico de la información, define el Plan de Tratamiento de Riesgos en Seguridad y Privacidad de la Información, Seguridad Digital con un enfoque en estrategia preventiva. Esto implica entender y manejar los riesgos relacionados con la interrupción de operaciones y el entorno digital. Se priorizan acciones para minimizar el impacto en la entidad en caso de que estos riesgos se materialicen. Además, el plan abarca la identificación, análisis, tratamiento, evaluación y monitoreo de riesgos de manera objetiva, destacando situaciones que puedan afectar la consecución de objetivos en áreas como el Desarrollo Digital, el empoderamiento ciudadano en el entorno digital, la Transformación Digital Sectorial y Territorial, y la Inclusión Social Digital.

Este enfoque cumple con la normativa colombiana, incluyendo el CONPES 3995 de 2020, el Modelo de Seguridad y Privacidad de MINTIC, y las disposiciones del decreto 1008 de 2018 y la Resolución 500 de 2021. Estas normativas establecen lineamientos y estándares para la seguridad digital, adoptando el modelo de seguridad y privacidad como parte esencial de la política de Gobierno Digital. El plan también se alinea con las buenas prácticas y los estándares internacionales ISO 27001, ISO 31000:2018, así como la guía para la administración del riesgo y el diseño de controles en entidades públicas, enfocándose en riesgos de gestión, corrupción y seguridad digital, de acuerdo con el Modelo Integrado de Planeación y Gestión

TABLA DE CONTENIDO

PRESENTACIÓN 2
1. OBJETIVO GENERAL 4
1.1. Objetivos Específicos 4
2. MARCO LEGAL 4
3. DEFINICIONES 5
4. DESARROLLO DEL PLAN 6
4.1. Metodología 6
Análisis de información 6
Identificación de riesgos 6
Valoración y análisis del riesgo 7
Control del riesgo 7
Monitoreo de riesgos 7
4.2. Actividades de Implementación 2024 7
5. SEGUIMIENTO 8
6. CONTROL DE CAMBIOS DEL DOCUMENTO 8
7. APROBACIÓN DEL DOCUMENTO 8

1. OBJETIVO GENERAL

Definir la ruta de trabajo para la gestión de riesgos de seguridad de la información/digital que, permita mantener la integridad, confidencialidad y disponibilidad de la información mediante la gestión de riesgos asociados a los activos de información Institucional.

1.1. Objetivos Específicos

- Identificar riesgos en cada uno de los procesos institucionales que afecten la triada de la información, basados en los activos de información reportados.
- Establecer e implementar controles específicos a través de planes.
- Reducir la probabilidad de materialización de los riesgos sobre los activos de información.
- Realizar seguimiento de los planes de manejo para el tratamiento de los riesgos.

2. MARCO LEGAL

- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012
- Decreto 1078 del 26 de mayo del 2015 “Por medio del cual se expide el Decreto único Reglamentario del Sector de Tecnologías de la Información y Comunicaciones”
- Decreto 1083 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.
- 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.
- Resolución 500 del 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”
- Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Departamento Administrativo de la Función Pública 2020.
- Guía de gestión del riesgo, Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)
- Modelo Nacional de Gestión de Riesgos de Seguridad Digital, Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)
- Guía de orientación para la Gestión de Riesgos de Seguridad Digital en el Gobierno Nacional, territoriales y sector público, Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)
- Norma Técnica Colombiana NTC-ISO-IEC 27001:2013
- Norma Técnica Colombiana NTC-ISO 31000:2011
- CONPES 3854 de 2016. Política Nacional de Seguridad digital

3. DEFINICIONES

- Aceptación del riesgo: Decisión informada de tomar un riesgo particular.
- Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de este.
- Causa: Origen, comienzo de una situación determinada que genera un efecto o consecuencia.
- Consecuencia: Resultado de un evento que afecta los objetivos.
- Control: Medida que modifica el riesgo.
- Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.
- Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).
- MSPI: Modelo de Seguridad y Privacidad de la Información
- Propietario del riesgo: Persona o Entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.
- Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.
- Riesgo: Efecto de la incertidumbre sobre los objetivos.
- Riesgo de Seguridad de la Información: Probabilidad de ocurrencia de un evento que genere un impacto sobre la Confidencialidad, Integridad y Disponibilidad de la Información.
- Valoración del riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.
- Tratamiento del Riesgo: Proceso para modificar el riesgo.
- Triada de la información: Conjunto de las propiedades derivadas de la Confidencialidad, Integridad y Disponibilidad de la Información.
- Vulnerabilidad: Debilidad de un activo que puede ser explotada por una o más amenazas.

4. DESARROLLO DEL PLAN

A continuación, se describe el ciclo que se ejecutará para la gestión de riesgos de seguridad de la información, siguiendo las metodologías publicadas por el DAFP y Min Tic, la cual será desarrollada a través de la ejecución de las actividades propuestas en el numeral 4.2

4.1. Metodología

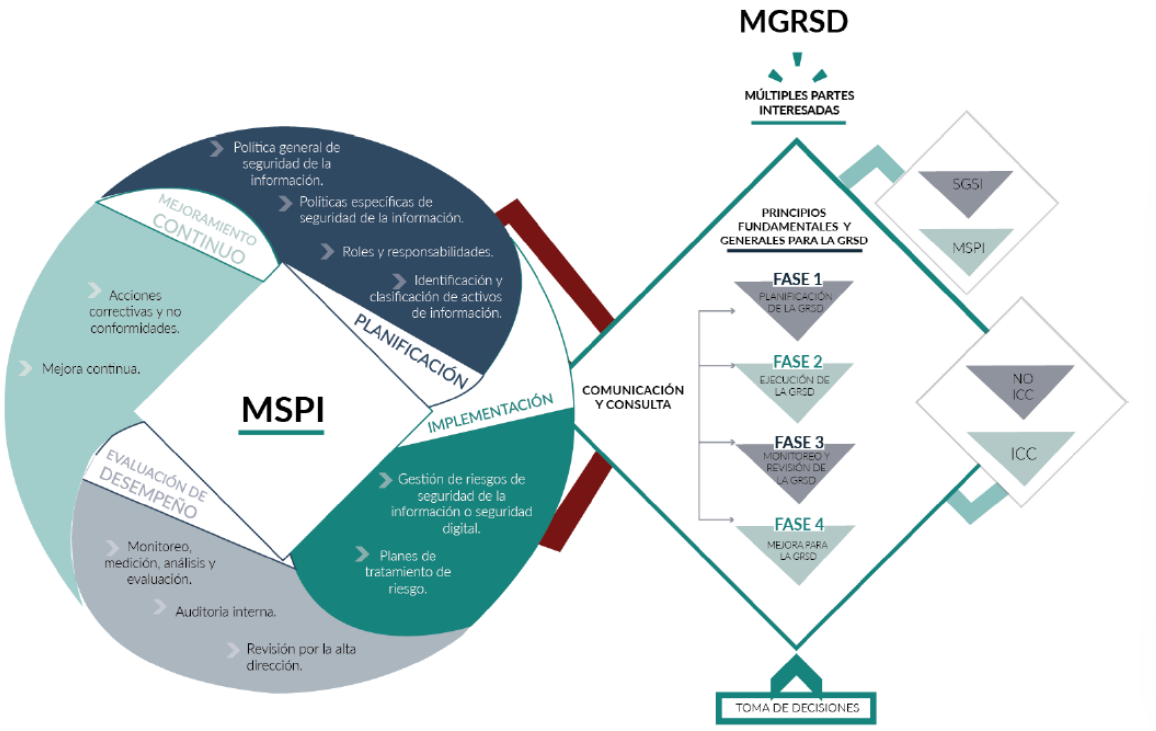

Ilustración 1 Interacción entre el MSPI y el MGRSD. Fuente: MinTIC

Análisis de información

La actividad inicial para la identificación será el levantamiento, clasificación y actualización de activos de información realizada por cada proceso institucional.

El líder del proceso deberá priorizar los activos con calificación en nivel alto registrados en el formato TIC-FR-010-y los demás que este considere para la generación de los riesgos.

Identificación de riesgos

Se identifican las amenazas, vulnerabilidades, consecuencias y se determina la probabilidad e impacto que puede llegar a afectar a uno o varios activos de información, interrumpiendo alguno de los elementos de la triada de información.

Valoración y análisis del riesgo

Se establecen los criterios para:

- Analizar el riesgo.
- Evaluar

Establece la probabilidad de ocurrencia y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgos inherente.

Control del riesgo

De acuerdo con los riesgos identificados se establecerán los controles que permitan mitigar/tratarlos, para ello la Entidad se basará en los propuestos en la NTC-ISO-IEC 27001:2022, esto con el fin de mitigar la materialización del riesgo asociados a los incidentes de seguridad.

Monitoreo de riesgos

De acuerdo con la periodicidad definida se revisarán los avances del plan de tratamiento de riesgos de seguridad de la información, analizando y verificando que las actividades establecidas en estos se estén llevando a cabo.

4.2. Actividades de Implementación 2024

Estrategia	Actividades	Evidencia
Revisión/actualización de documentación	Actualizar manual de gestión de riesgos de seguridad digital.	Documento TIC-MA-007 publicado y aprobado
Concienciación sobre conceptos y bases para la identificación de riesgos	Elaborar pieza gráfica relacionada con tips para identificación de riesgos.	Piezas gráficas y correo electrónico con envío masivo.
Identificación de riesgos de seguridad de la información	Solicitar revisión, identificación y gestión sobre los riesgos en las áreas	Memorando con solicitud
	Identificar, analizar y evaluar los riesgos de seguridad para todos los procesos de la cadena de valor	Matriz de riesgos
	Revisar, validar y ajustar los riesgos.	
Plan de tratamiento de riesgos de seguridad de la información	Documentar las actividades relacionadas para implementar los controles establecidos.	Plantilla en Excel para reporte de riesgos.
Aceptación del riesgo de seguridad de la información	Consolidar las aprobaciones de las matrices de riesgos de seguridad por el propietario del riesgo (líder del proceso) como declaración formal de la aceptación	Correo electrónico/memorando
Seguimiento planes de tratamiento de riesgos de seguridad de la información	Revisar la documentación y evidencias de los seguimientos realizados al plan de tratamiento	Correo electrónico, Actas de sesiones

Estrategia	Actividades	Evidencia
Mejoramiento	Identificar oportunidades de mejora conforme los resultados de la evaluación del riesgo residual	Correo electrónico, Actas de sesiones
Monitoreo	Reporte de actividades de seguimiento a través del plan e indicadores	Archivo de seguimiento.

5. SEGUIMIENTO

La dependencia encargada de realizar el monitoreo, seguimiento y control del plan de acuerdo con la competencia y la normatividad vigente es la Oficina de Tecnologías de la información y las comunicaciones.

6. CONTROL DE CAMBIOS DEL DOCUMENTO

Control de cambios		
Versión	**Fecha**	**Descripción del cambio**
1	20-Ene-2022	Creación del documento
2	20-Dic-2022	Actualización de actividades
3	20-Dic-2023	Actualización de introducción y actividades; se incorpora estrategia de monitoreo.

7. APROBACIÓN DEL DOCUMENTO

Aprobación del documento		
Etapa	**Nombres y apellidos**	**Cargo**
Elaboro	Maria Alejandra Suarez	Contratista
Aprobó	Miembros con voto	Comité Institucional de Gestión y Desempeño