SUPERINTENDENCIA
DE SOCIEDADES

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

1. INTRODUCCIÓN

La Superintendencia de Sociedades, en el marco del Modelo Integrado de Planeación y Gestión MIPG, y sus políticas de Gobierno Digital y Seguridad Digital, políticas que dinamizan la gestión institucional, orientadas respectivamente a promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones, para consolidar la relación TIC para el Estado y la relaciónTIC para la sociedad; y así mismo, gestionar adecuadamente los riesgos de seguridad y privacidad de la información, en aras de la preservación de la confidencialidad, la integridad y la disponibilidad de la información, atenderá lo dispuesto en el presente plan.

De igual forma, y dando cumplimiento a la normatividad establecida por el estado colombiano, tal como lo define el CONPES 3854 de 2016, el 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 - Versión 5 de diciembre de 2020, emitida por el Departamento Administrativo de la Función Pública DAFP; la Superintendencia de Sociedades ha definido el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, en el que se determinan las actividades, responsables y fechas orientadas a gestionar un adecuado proceso de administración de riesgos de seguridad y privacidad de la información.

2. OBJETIVO

Definir e implementar una hoja de ruta que permita a la Entidad gestionar los riesgos de seguridad y privacidad de la información, desde la misma identificación de sus activos de seguridad de la información, y con base en ellos, la identificación de sus riesgos, su valoración, establecimiento de controles y el respectivo seguimiento, atendiendo los lineamientos normativos e institucionales, dispuestos en los siguientes documentos: “Instructivo para la Identificación, Clasificación/Valoración y Etiquetado de Activos de Información” GC-I-001, y el “Instructivo para la Gestión de Riesgos de Seguridad de la Información” GC-C-002.

3. ALCANCE

Los lineamientos establecidos en este Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, aplican a todos los procesos y sedes regionales de la Superintendencia de Sociedades, y contemplan todas las acciones orientadas a fortalecer sus capacidades institucionales en materia de riesgos de seguridad y privacidad de la información y su adecuada gestión.

4. ACTIVIDADES A DESARROLLAR

ACTIVIDAD	RESPONSABLE(S)	FECHA DE INICIO	FECHA FIN
Revisión y actualización de los lineamientos de riesgos de seguridad y privacidad de la información (Política de seguridad de la información y/o, modelos y demás políticas y lineamientos en esta materia).	Oficina Asesora de Planeación. Dirección de Tecnología de la Información y las Comunicaciones.	01 de febrero de 2022	31 de diciembre de 2022
Identificación y actualización de riesgos y controles de seguridad y privacidad de la información.	Líderes de proceso e Intendencias.	17 de enero 2022	30 de junio de 2022
Monitoreo y seguimiento a la gestión de los riesgos de seguridad y privacidad de la información.	Líderes de proceso e Intendencias.	01 de julio de 2022	30 de septiembre de 2022
Actualización de los activos de seguridad de la información.	Líderes de proceso e Intendencias.	01 de octubre de 2022	31 de diciembre de 2022
Sensibilización.	Oficina Asesora de Planeación. Dirección de Tecnología de la Información y las Comunicaciones. Líderes de proceso e Intendencias.	01 de febrero de 2022	31 de diciembre de 2022

4.1 Revisión y actualización de los lineamientos de riesgos de seguridad y privacidad de la información (Política de seguridad de la información y/o, modelos y demás políticas y lineamientos en esta materia).

Se llevará a cabo la revisión de la política de seguridad de la información, implícita en la Política del Sistema de Gestión Integrado, conforme a lo exigido por los lineamientos normativos. Se continuará con la revisión de los modelos y políticas, en el marco de lo establecido por el Sistema de Gestión de Seguridad de la Información SGSI, y del Modelo de Seguridad y Privacidad de la Información MSPI. Se actualizarán aquellas que así lo requieran.

4.2 Identificación y actualización de riesgos y controles de seguridad y privacidad de la información.

Con base en la actualización de los activos de seguridad de la información, realizada en el segundo semestre de 2021, se llevará a cabo la actualización de riesgos y controles de seguridad de la información, atendiendo los lineamientos establecidos en el “Instructivo para la Identificación, Clasificación/Valoración y Etiquetado de Activos de Información” GC-I-001, y el “Instructivo para la Gestión de Riesgos de Seguridad de la Información” GC-C-002.

4.3 Monitoreo y seguimiento a la gestión de los riesgos de seguridad y privacidad de la información.

Atendiendo el esquema de líneas de defensa, establecido por el Modelo Integrado de Planeación y Gestión MIPG, la línea estratégica conformada por la Alta Dirección de la Entidad y el equipo directivo, a través de sus comités define el marco general para la gestión del riesgo y control y supervisa su cumplimiento y toma decisiones para la mejora.

Corresponde a los líderes de procesos e intendentes regionales, como primera línea de defensa, diseñar, implementar y monitorear los controles, además de gestionar de manera directa en el día a día los riesgos de la Entidad.

La Oficina Asesora de Planeación, en su rol de segunda línea de defensa, realizará la labor de seguimiento, con el fin de evidenciar de que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados adecuadamente y funcionen como es debido. Su rol consiste en monitorear la gestión del riesgo y control ejecutada por la primera línea de defensa.

La tercera línea de defensa, a cargo de la Oficina de Control Interno, proporciona información sobre la efectividad del Sistema de Control Interno, a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa. Lo anterior, basado en el más alto nivel de independencia y objetividad sobre la efectividad del Sistema de Control Interno SCI.

4.4 Actualización activos de seguridad de la información.

En esta etapa, se revisarán y si se requiere, se actualizarán los activos de seguridad de la información por proceso e intendencia regional, atendiendo las directrices normativas, institucionales y oportunidades de mejora establecidas para dicha gestión.

4.5 Sensibilización.

Actividad orientada a la toma de conciencia y apropiación, por parte de los funcionarios, contratistas y terceros de la Entidad frente a la gestión de riesgos de seguridad y privacidad de la información, a través de capacitaciones, foros, charlas, campañas, entre otros, haciendo uso de las herramientas de comunicaciones disponibles en la Entidad.

5. RECURSOS

El desarrollo de las actividades estará sujeto a la disponibilidad de recursos (humanos, tecnológicos, financieros, entre otros) que faciliten el cumplimiento de las actividades.

RECURSO	DESCRIPCIÓN
Humano	Profesionales de la Oficina Asesora de Planeación y la Dirección de Tecnología de la Información y las Comunicaciones, quienes llevarán a cabo labores de asesoría a Líderes de Proceso, Intendentes y Colaboradores en materia de riesgos de seguridad y privacidad de la información. Gestores de Riesgo, quienes deberán aplicar y transferir conocimiento al interior de sus procesos e intendencias, al respecto de los lineamientos

	impartidos por los Profesionales de la Oficina Asesora de Planeación y la Dirección de Tecnología de la Información y las Comunicaciones. Líderes de Proceso e Intendentes, como actores principales de la primera línea de defensa, deberán acoger e implementar los lineamientos en el marco de la gestión de riesgos de seguridad y privacidad de la información. Línea Estratégica y/o Alta Dirección, aprobarán, supervisarán y tomarán decisiones, con respecto a la gestión institucional en esta materia. La Oficina de Control Interno, evaluará la gestión del riesgo de seguridad y privacidad de la información. Funcionarios, contratistas, proveedores y terceros en general, acogerán y aplicarán los lineamientos en lo concerniente a la seguridad y privacidad de la información.
Tecnológicos	Aplicativos, sistemas y aplicaciones para la gestión de los riesgos de seguridad y privacidad de la información (entre ellos el Aplicativo Riesgos y Auditoría, correo electrónico, TEAMS, sharepoint, entre otros).
Normativos y reglamentarios	Guías, Modelos, Políticas, Sistemas de Gestión, etc, que orientan la gestión e implementación de los riesgos de seguridad y privacidad de la información.
Financieros	Recursos orientados para la adquisición de conocimiento, recursos humanos, tecnológicos, entre otros.