

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
2025

SUPERINTENDENCIA DE VIGILANCIA Y SEGURIDAD PRIVADA

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Oficina de Sistemas – Seguridad de la Información	Gestión de Sistemas e Información
Revisó y Aprobó	Juan Gabriel Pérez Tobaría – Jefe Oficina de Sistemas (e)	Gestión de Sistemas e Información

TABLA DE CONTENIDO

1.

NTRODUCCIÓN

2

2.

OBJETIVO

3

2.1.

Objetivos Específicos

3

3.

ALCANCE

3

4.

DEFINICIONES

4

5.

MARCO LEGAL

5

6.

DESARROLLO

7

7.

RESPONSABILIDAD:

8

1. NTRODUCCIÓN

La Superintendencia de Vigilancia y Seguridad Privada, en cumplimiento de la normatividad vigente, ha diseñado el presente Plan de Seguridad y Privacidad de la Información. Este plan se enmarca en la implementación de la Política de Gobierno Digital, establecida en el Decreto 767 de 2022 y compilada en el Decreto Único Reglamentario del Sector TIC, 1078 de 2015.

La Política de Gobierno Digital y Seguridad Digital tiene como propósito promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital. Uno de los habilitadores fundamentales de esta política es la Seguridad y Privacidad de la Información, que busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

En este contexto, la Superintendencia de Vigilancia y Seguridad Privada ha adoptado el Modelo de Seguridad y Privacidad de la Información (MSPI) expedido por el Ministerio de Tecnologías de Información y de las Comunicaciones, con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información, apoyada en un proceso de gestión del riesgo que brinde confianza a las partes interesadas.

Este documento presenta el Plan de Seguridad y Privacidad de la Información de la Superintendencia de Vigilancia y Seguridad Privada, que define los lineamientos, estrategias y actividades a implementar para garantizar la adecuada gestión de la seguridad y privacidad de la información en la entidad.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Oficina de Sistemas – Seguridad de la Información	Gestión de Sistemas e Información
Revisó y Aprobó	Juan Gabriel Pérez Tobaría – Jefe Oficina de Sistemas (e)	Gestión de Sistemas e Información

2. OBJETIVO

Establecer las estrategias y actividades orientadas a fortalecer la gestión de la seguridad y privacidad de la información generada, tratada y custodiada por la Superintendencia de Vigilancia y Seguridad Privada, con el fin de preservar su confidencialidad, integridad y disponibilidad, en cumplimiento de la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI) y el marco legal aplicable, para generar confianza en los grupos de interés.

2.1. Objetivos Específicos

El Plan de Seguridad y Privacidad de la Información da cumplimiento al objetivo general a través de los siguientes objetivos específicos:

- Consolidar el Sistema de Gestión de Seguridad de la Información (SGSI) de la Superintendencia, mediante la implementación y mejora de los controles de seguridad establecidos en el MSPI, alineados con la norma NTC ISO/IEC 27001:2022.
- Definir y divulgar a los colaboradores de la entidad, las políticas, documentación asociada y buenas prácticas que permitan fortalecer la cultura institucional en torno a la seguridad y privacidad de la información.
- Realizar el seguimiento y evaluación de las acciones orientadas a reducir las brechas de cumplimiento de la Política de Gobierno Digital, de acuerdo con los resultados del autodiagnóstico del Modelo Integrado de Planeación y Gestión (MIPG).
- Garantizar el cumplimiento de los requisitos legales y normativos en materia de seguridad y privacidad de la información, gobierno digital y protección de datos personales.

3. ALCANCE

El presente Plan de Seguridad y Privacidad de la Información aplica a todos los procesos identificados en el modelo de operación por procesos de la Superintendencia de Vigilancia y Seguridad Privada, involucrando a todos los funcionarios, contratistas, proveedores y terceros que, en el cumplimiento de sus funciones, compartan, utilicen, recolecten, procesen, intercambien o consulten la información de la entidad.

De esta manera, el alcance del plan abarca:

- Todos los procesos, trámites, servicios, sistemas de información, infraestructura y, en general, todos los activos de información de la Superintendencia.
- Todos los funcionarios, tanto de planta como contratistas, que tengan acceso y manipulen información de la entidad.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Oficina de Sistemas – Seguridad de la Información	Gestión de Sistemas e Información
Revisó y Aprobó	Juan Gabriel Pérez Tobaría – Jefe Oficina de Sistemas (e)	Gestión de Sistemas e Información

- Todos los proveedores y terceros que, en el marco de sus contratos o acuerdos, interactúen con la información de la Superintendencia.
- Cualquier persona o entidad que, por razones del cumplimiento de sus funciones, tenga acceso y haga uso de la información de la Superintendencia de Vigilancia y Seguridad Privada.
- El plan busca establecer los lineamientos, estrategias y actividades necesarias para preservar la confidencialidad, integridad y disponibilidad de la información, en cumplimiento de la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI) y el marco normativo aplicable.

4. DEFINICIONES

- **Activos de Información:** Se refiere a cualquier información o elemento que tiene valor estratégico para los procesos de negocio de la Agencia Nacional de Seguridad Vial.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
- **Control:** Medida que permite reducir o mitigar un riesgo.
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
- **Integridad:** Propiedad de exactitud y completitud.
- **MIPG:** Modelo Integrado de Planeación y Gestión.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información.
- **Seguridad de la información:** Conjunto de medidas que toman las personas y las organizaciones, que les permiten resguardar y proteger los activos de información, preservando su confidencialidad, integridad y disponibilidad.
- **Sistema de Gestión de Seguridad de la información (SGSI):** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una institución para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Oficina de Sistemas – Seguridad de la Información	Gestión de Sistemas e Información
Revisó y Aprobó	Juan Gabriel Pérez Tobaría – Jefe Oficina de Sistemas (e)	Gestión de Sistemas e Información

5. MARCO LEGAL

- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado de la protección de la información y de los datos- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- 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.
- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- Ley 1702 de 2013. Por la cual se crea la Agencia Nacional de Seguridad Vial 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 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 1499 de 2017. Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión.
- Decreto 1008 del 2018. 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.
- Resolución 025 de 2020. Por la cual se adopta la Política de Seguridad y Privacidad de la Información y se definen lineamientos para su uso, actualización y aplicación.
- CONPES 3854 de 2016. Política Nacional de Seguridad Digital.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Oficina de Sistemas – Seguridad de la Información	Gestión de Sistemas e Información
Revisó y Aprobó	Juan Gabriel Pérez Tobaría – Jefe Oficina de Sistemas (e)	Gestión de Sistemas e Información

- CONPES 3975 DE 2019 Política Nacional para la Transformación Digital e Inteligencia Artificial.
- 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 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 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.
- Directiva Presidencial 03 de 2021. Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
- Resolución 460 de 2022 - Ministerio de Tecnologías de la Información y las Comunicaciones. Por la 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.
- Circular 01 de 2022 - Departamento Administrativo de la Presidencia de la República. Recomendaciones de uso de servicios en la nube como medida para mitigar riesgos de seguridad digital.
- Decreto 255 de 2022 - Ministerio de Comercio, Industria y Turismo. Por el cual se adiciona la Sección 7 al Capítulo 25 del Título 2 de la Parte 2 del Libro 2 de/ Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, sobre normas corporativas vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países.
- Directiva 02 de 2022 - Presidencia de la República. Reiteración de la política pública en materia de seguridad digital.
- Decreto 338 de 2022 - Ministerio de Tecnologías de la Información y las Comunicaciones. Por el cual se adiciona el Título 21 a la 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.
- Resolución 746 de 2022 - Ministerio de Tecnologías de la Información y las Comunicaciones. Por la 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.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Oficina de Sistemas – Seguridad de la Información	Gestión de Sistemas e Información
Revisó y Aprobó	Juan Gabriel Pérez Tobaría – Jefe Oficina de Sistemas (e)	Gestión de Sistemas e Información

- Resolución 01117 de 2022 - Ministerio de Tecnologías de la Información y las Comunicaciones. 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 7870 de 2022 Ministerio de Defensa Nacional – Política General de seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y Continuidad de los Servicios Tecnológicos en la Unidades Ejecutoras o Dependencias del Ministerio de Defensa Nacional, Policía Nacional y entidades adscritas y vinculadas al Sector Defensa
- Decreto 767 de 2022 - Presidencia de la República. 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.
- Ley 2294 de 2023 – Plan Nacional de Desarrollo 2022- 2026 “Colombia potencia mundial de la vida”. Artículo 143. Transformación digital como motor de oportunidades e igualdad. Numeral 4.

6. DESARROLLO

La Oficina de Sistemas de la SVSP establece las siguientes actividades para la implementación del El Modelo de Seguridad y Privacidad de la Información MSPI.

Gestión de Seguridad de la Información



	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Oficina de Sistemas – Seguridad de la Información	Gestión de Sistemas e Información
Revisó y Aprobó	Juan Gabriel Pérez Tobaría – Jefe Oficina de Sistemas (e)	Gestión de Sistemas e Información

7. CRONOGRAMA DE ACTIVIDADES

La Oficina de Sistemas de la SVSP establece las siguientes actividades para la vigencia 2025.

OBJETIVO	Implementar, mantener y mejorar el Sistema de Gestión de Seguridad de Información - SGSI basado en la política de Gobierno Digital y la norma ISO/IEC 27001:2022, alineado al cumplimiento de los objetivos estratégicos de la SuperVigilancia, buscando proteger la Confidencialidad, Integridad y Disponibilidad de la información en la SuperVigilancia.	ALCANCE	Aplica para todos servidores públicos, contratistas y terceros, que hacen uso de los recursos y activos de información de la SuperVigilancia, así como a los designados para su uso y custodia, siendo de obligatorio cumplimiento.
META	Cumplir el 90% de las actividades propuestas en la implementación del SGSI de conformidad con la ISO 27001:2022	FECHA DE ELABORACION	Abril 1 2025

No.	ACTIVIDAD	RESPONSABLE	AÑO: 2025												RECURSOS			ENTREGABLE	OBSERVACIONES
			1	2	3	4	5	6	7	8	9	10	11	12	T	H	F		
1	Gestión de Incidentes de Seguridad de la Información	Oficina de Sistemas				11%	11%	11%	11%	11%	11%	11%	11%	12%	100%	x	x	Seguimiento y gestión a incidentes de seguridad de la información que se Presenten	
2	Revisar e Implementar, si aplica recomendaciones de seguridad recibidas de AUTORIDADES - GRUPOS ESPECIALES DE INTERES - INTELIGENCIA DE AMENAZAS	Oficina de Sistemas				11%	11%	11%	11%	11%	11%	11%	11%	12%	100%	x	x	Implementación de controles recomendados y que apliquen a la SVSP	
3	Análisis y remediación de vulnerabilidades	Oficina de Sistemas						50%					50%		100%	x	x	Informe de vulnerabilidades identificadas y acciones realizadas	
4	Gestión y monitoreo de los activos de seguridad de TI	Oficina de Sistemas				20%		30%		20%		30%			100%	x	x	Reporte periódico de disponibilidad de los servicios e infraestructura	
5	Actividades de control sobre elementos de la infraestructura de seguridad	Oficina de Sistemas			20%		20%		20%		20%		20%		100%	x	x	Ajustes sobre la Infraestructura de seguridad derivados del reporte de disponibilidad	
6	Capacitaciones en Seguridad de la Información	Oficina de Sistemas		30%					30%					40%	100%	x		Charlas a los funcionarios y contratistas de la Superintendencia en temas relacionados con seguridad de la información	
7	Tips de seguridad de la información	Oficina de Sistemas			10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	100%	x	x	Pantallas o piezas graficas de Tips de seguridad enviados	
8	Evaluación del SGSI	Oficina de Sistemas				90%							10%		100%	x		Autoevaluación del SGSI	

ELABORADO: Miguel Antonio García Arango Seguridad de la Información - Oficina de Sistemas

APROBADO: Juan Gabriel Perez Tobaría - Jefe Oficina de Sistemas (e).

FECHA DE APROBACIÓN: Abril 1 2025

8. RESPONSABILIDAD:

Este documento y la ejecución de las actividades es responsabilidad de la Oficina de Sistemas de la Superintendencia de Vigilancia y Seguridad Privada.

Cordialmente,



Juan Gabriel Pérez Tobaría
Jefe Oficina de Sistemas (e)

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Oficina de Sistemas – Seguridad de la Información	Gestión de Sistemas e Información
Revisó y Aprobó	Juan Gabriel Pérez Tobaría – Jefe Oficina de Sistemas (e)	Gestión de Sistemas e Información