



Superservicios
Superintendencia de Servicios
Públicos Domiciliarios

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



Oficina Asesora de Planeación e Innovación Institucional

Enero, 2023 V.1

1. OBJETIVO

Establecer las actividades orientadas a fortalecer el tratamiento de la información que es generada, tratada y custodiada por la entidad; con el fin de elevar su nivel de confianza con sus grupos de interés, mediante la preservación de su confidencialidad, integridad y disponibilidad, así como también la adopción de las buenas prácticas, el cumplimiento de la política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información y el marco legal que le sea aplicable.

1.1 OBJETIVOS ESPECÍFICOS

- Fortalecer el Sistema de Gestión de Seguridad y Privacidad de la Información (SIGESPI) de la entidad, mediante la implementación y mejora de los controles de seguridad establecidos en el Modelo de Seguridad y Privacidad de la información (MSPI), los cuales se encuentran alineados con el Anexo A de la norma NTC ISO/IEC 27001:2013.
- Definir y divulgar a los colaboradores de la entidad, las políticas, documentación asociada y buenas prácticas que permitan consolidar una cultura institucional en torno a la seguridad de la Información.
- Realizar el seguimiento a las acciones que permitan reducir las brechas de cumplimiento de la Política de Gobierno Digital con el autodiagnóstico del Modelo Integrado de Planeación y Gestión (MIPG), frente a relacionado con el habilitador transversal de seguridad y privacidad de información.
- Dar cumplimiento a los requisitos legales y normativos en materia de seguridad y privacidad de la información, gobierno digital y protección de datos personales.

2. DEFINICIONES

- **Activo de información:** En el contexto de seguridad digital son elementos tales

como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

- **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 y privacidad de la información (SIGESPI):** 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.

3. MARCO LEGAL

- **Ley 527 de 1999.** Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- **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 1437 de 2011, Capítulo IV.** "Utilización de medios electrónicos en el procedimiento administrativo". "Los procedimientos y trámites administrativos podrán realizarse a través de medios electrónicos. Para garantizar la igualdad de acceso a la administración, la autoridad deberá asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros procedimientos."
- **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 886 de 2014.** Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- **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 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. Parte 1 - Disposiciones reglamentarias generales. Título 1 - Disposiciones generales en materia de transparencia y del derecho de acceso a la

información pública nacional.

- **Decreto 103 de 2015.** Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 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.
- **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.
- **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. Artículos 1 y 2 relacionados con el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan de Seguridad y Privacidad de la Información.
- **CONPES 3975 de 2019.** Política nacional para la transformación digital e inteligencia artificial.
- **Ley 1955 de 2019.** Por el cual se expide el Plan Nacional de Desarrollo 2018-2022. “Pacto por Colombia, Pacto por la Equidad”. Artículo 147. Transformación Digital Pública. Las entidades estatales del orden nacional deberán incorporar en sus respectivos planes de acción el componente de transformación digital siguiendo los estándares que para este propósito defina el Ministerio de Tecnologías de la Información y las Comunicaciones. Artículo 148. Gobierno Digital como Política de Gestión y Desempeño Institucional. Todas las entidades de la administración pública deberán adelantar las acciones que señale el Gobierno nacional a través del Ministerio de Tecnologías de la Información y las Comunicaciones para la implementación de la política de Gobierno Digital.
- **CONPES 3995 de 2019.** Política nacional de confianza y 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 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.
- **Decreto Presidencial 88 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.
- **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.
- **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.
- **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.

4. ALCANCE

El alcance del Plan de Seguridad y Privacidad de la Información aplica para todos los procesos identificados en el modelo de operación institucional, a todos sus funcionarios, contratistas, proveedores y aquellas personas o terceros que para el cumplimiento de sus funciones y las de la entidad, compartan, utilicen, recolecten, procesen, intercambien o consulten su información.

5. PLANIFICACIÓN DE ACTIVIDADES

ACTIVIDAD	RESPONSABLE ¹	FECHA INICIO	FECHA FIN
Revisar y de ser necesario actualizar el Instructivo para la identificación y clasificación de activos de información.	Oficial de seguridad de la información	1/04/2023	30/04/2023
Actualizar la información contenida en el Registro Nacional de Bases de Datos de la Superintendencia de Industria y Comercio, teniendo en cuenta la información suministrada por los procesos de la entidad.	Oficial de protección de datos personales	1/03/2023	31/03/2023
Actualizar en la plataforma de la Superintendencia de Industria y Comercio la información de los reclamos presentados por los titulares relacionados con la protección de datos personales.	Oficial de protección de datos personales	1/02/2023	31/08/2023
Realizar seguimiento a los incidentes de Ciberseguridad y Privacidad de la Información que se presenten en la entidad.	Oficial de seguridad de la información	31/03/2023 30/06/2023 30/09/2023 31/12/2023	
Revisar, y de ser necesario actualizar, las políticas complementarias de Seguridad y	Oficial de seguridad de la información	1/03/2023	30/09/2023

¹ Los roles de Oficial de Seguridad de la Información y el de Protección de Datos Personales fueron asignado al jefe de la Oficina Asesora de Planeación e Innovación Institucional, de acuerdo con la Resolución No. SSPD – 20211000576955 del 12/10/2021.

ACTIVIDAD	RESPONSABLE¹	FECHA INICIO	FECHA FIN
Privacidad de la Información.			
Revisar y actualizar la documentación del Sistema Integrado de Gestión y Mejora -SIGME relacionada con la información que involucra los temas de protección de datos personales y ley de transparencia.	Oficial de seguridad de la información – Oficina de administración de riesgos y estrategias de supervisión – Superintendencias Delegadas de Energía y gas Combustible y de Acueducto, Alcantarillado y Aseo	1/04/2023	30/04/2023
Elaborar o ajustar documentos que complementen las políticas del Sistema Integrado de Gestión de Seguridad y Privacidad de la Información -SIGESPI o apoyar metodológicamente a las otras dependencias en la construcción de los mismos.	Oficial de seguridad de la información – Oficina de Tecnologías de la Información y las Comunicaciones	1/04/2023	31/08/2023
Realizar actividades de toma de conciencia en materia de seguridad de la información, protección de datos personales y continuidad de negocio.	Oficial de seguridad de la información y Oficial de protección de datos personales	1/01/2023	31/12/2023
Asesorar metodológicamente la construcción del Plan de Contingencia del Sistema de Gestión Documental Electrónico y de Archivo - SGDEA que posee la entidad.	Oficial de seguridad de la información	1/06/2023	30/06/2023
Realizar la prueba que permita validar el Plan de Contingencia	Oficial de seguridad de la información	1/10/2023	31/10/2023

ACTIVIDAD	RESPONSABLE¹	FECHA INICIO	FECHA FIN
relacionado con el Sistema de Gestión Documental Electrónico y Archivo –SGDEA, que posee la entidad.			
Asesorar metodológicamente la construcción del Plan de Contingencia de un sistema de información crítico definido en el ejercicio de Análisis de Impacto de Negocio.	Oficial de seguridad de la información	1/11/2023	30/11/2023
Actualizar el Plan de Recuperación ante Desastres - DRP.	Oficina de Tecnologías de la Información y las Comunicaciones	1/09/2023	30/09/2023
Definir los criterios de auditoría y trazabilidad para los componentes y sistemas de información críticos definidos, como parte del dominio de arquitectura de seguridad del modelo de Arquitectura Empresarial.	Oficial de seguridad de la información - Oficina de Tecnologías de la Información y las Comunicaciones	1/06/2023	30/11/2023
Integrar en la estrategia conceptual de inteligencia institucional el componente de seguridad y privacidad de la información.	Oficial de seguridad de la información – Oficina de administración de riesgos y estrategias de supervisión – Superintendencias Delegadas de Energía y gas Combustible y de Acueducto, Alcantarillado y Aseo - Oficina de Tecnologías de la Información y las	1/07/2023	31/08/2023

 Superservicios Superintendencia de Servicios Públicos Domiciliarios	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	 SIGME
--	--	---

ACTIVIDAD	RESPONSABLE ¹	FECHA INICIO	FECHA FIN
	Comunicaciones		
Realizar las evaluaciones de vulnerabilidades sobre la infraestructura T.I. y monitorear los planes de remediación que se vayan a implementar.	Oficina de Tecnologías de la Información y las Comunicaciones	28/02/2023 30/04/2023 31/07/2023 31/10/2023 31/12/2023	
Monitorear la gestión de vulnerabilidades sobre la infraestructura T.I.	Oficial de seguridad de la información	28/02/2023 30/04/2023 31/07/2023 31/10/2023 31/12/2023	
Participar en la auditoría interna programada por la Oficina Asesora de Planeación e Innovación Institucional, asociada al Sistema de Gestión de Seguridad y Privacidad de la Información.	Oficial de seguridad de la información - Oficina de Tecnologías de la Información y las Comunicaciones	1/07/2023	31/07/2023

CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
1	30/01/2022	Edición inicial