Superservicios
Superintendencia de Servicios Públicos Domiciliarios

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SIGME

Oficina Asesora de Planeación e Innovación Institucional
Julio, 2022 V.2

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 esta-tales del orden nacional deberán incorporar en sus respectivos planes de acción el componente de transformación digital siguiendo los es-tándares que para este propósito defina el Ministerio de

Tecnologías de la Información y las Comunicaciones. Artículo 148. Gobierno Digital como Política de Gestión y Desem-peño 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.

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

ACTIVIDADES	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	01/01/2022	28/02/2022
Socializar con los líderes de proceso y la Oficina Asesora Jurídica, los activos de información identificados y clasificados, para su respectiva aprobación.	Oficial de seguridad de la información	01/03/2022	31/05/2022
Publicar el inventario y los instrumentos de activos de información consolidado, previa aprobación del equipo temático de la Política de Transparencia.	Oficial de seguridad de la información	01/06/2022	29/07/2022

[1] El rol de Oficial de Seguridad de la Información y el rol de Oficial de Protección de Datos Personales fueron asignados al jefe de la Oficina Asesora de Planeación e Innovación Institucional, de acuerdo con la Resolución No. SSPD - 20201000042075 del 05/10/2020.

ACTIVIDADES	RESPONSABLE[1]	FECHA INICIO	FECHA FIN
Actualizar la información contenida en el Registro Nacional de Bases de Datos de la SIC, teniendo en cuenta la información suministrada por los procesos de la entidad.	Oficial de protección de datos personales	01/03/2022	31/03/2022
Actualizar en la plataforma de la SIC la información de los reclamos presentados por los titulares relacionados con la protección de datos personales.	Oficial de protección de datos personales	01/02/2022	31/08/2022
Realizar seguimiento a los incidentes de Ciberseguridad y Privacidad de la Información que se presenten en la entidad.	Oficial de seguridad de la información	31/03/2022 30/06/2022 30/09/2022 31/12/2022	
Articular la gestión de incidentes de seguridad de la información y seguridad informática con la mesa de ayuda.	Oficial de seguridad de la información - OTIC	02/05/2022	31/05/2022
Revisar, y de ser necesario actualizar, las políticas complementarias de Seguridad y Privacidad de la Información[2].	Oficial de seguridad de la información	01/05/2022	30/06/2022
Elaborar documentos (instructivos, procedimientos) que complementen las políticas del SIGESPI o apoyar metodológicamente a las otras dependencias en la construcción de los mismos (desarrollo, intercambio de información, control de accesos, OWASP)	Oficial de seguridad de la información - OTIC	01/02/2022	31/07/2022
Realizar actividades de toma de conciencia en materia de seguridad de la información y la protección de datos personales.	Oficial de seguridad de la información y Oficial de protección de datos personales	01/01/2022	31/12/2022
Documentar los planes alternos de operación	Oficial de seguridad de la información	01/03/2022	30/06/2022

[2] DE-M-004 Manual de políticas complementarias del SIGESPI
http://sigmecalidad.superservicios.gov.co/SSPD/Isodoc/consultas.nsf/442a1ae7d450e3b40525776900631052/f211a14dcd3c2ea4052587600073f08a?OpenDocument

ACTIVIDADES	RESPONSABLE[1]	FECHA INICIO	FECHA FIN
Identificar información inicial de continuidad de negocio	Oficial de seguridad de la información	01/05/2022	30/06/2022
Establecer el Plan de Recuperación ante Desastres (DRP).	OTIC	01/08/2022	30/09/2022
Apoyar los ejercicios de AE respecto al dominio de Arquitectura de Seguridad en cuanto a revisar (mantener, adicionar o ajustar) los controles técnicos definidos en el MSPI para asegurar la protección de la información mediante un enfoque de arquitectura, por ejemplo: - Definir sobre los sistemas de información los criterios para asegurar la trazabilidad y auditoría (registro histórico) en las acciones de creación, actualización, modificación o borrado de los componentes de información. - Analizar e incorporar aquellos componentes de seguridad y privacidad de la información que sean necesarios durante todas las fases del ciclo de vida de los sistemas de información. - Realizar la evaluación y tratamiento de los riegos de seguridad de la información asociados a su infraestructura tecnológica, aplicaciones y componentes de información.	Oficial de seguridad de la información - OTIC	01/03/2022	31/08/2022
Realizar las evaluaciones de vulnerabilidades sobre la infraestructura T.I. y monitorear los planes de remediación que se vayan a implementar.	OTIC	31/03/2022 30/06/2022 30/09/2022 31/12/2022	
Monitorear la gestión de vulnerabilidades sobre la infraestructura T.I.	Oficial de seguridad de la información	31/03/2022 30/06/2022 30/09/2022 31/12/2022	
Participar en la auditoría interna programada por la Oficina de Control Interno o la OAPII, asociada al SIGESPI.	Oficial de seguridad de la información - OTIC	01/07/2022	29/07/2022

ACTIVIDADES	RESPONSABLE[1]	FECHA INICIO	FECHA FIN
Implementar los certificados de seguridad de las aplicaciones web.	OTIC	01/07/2022	29/07/2022

CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
1	28/01/2022	Edición inicial
2	14/07/2022	Se amplió la fecha de la actividad: *"Publicar el inventario y los instrumentos de activos de información consolidado previa aprobación del equipo temático de la Política de Transparencia."*, a julio 29 de 2022, para realizar la actualización de los nombres de las series asignados a los activos de información de acuerdo con la Tabla de Retención Documental de 2021 y presentar nuevamente los instrumentos de acceso a la información pública al equipo temático de la Política de Transparencia para su aprobación respectiva.