1. OBJETIVO

Establecer las actividades necesarias requeridas para adelantar la gestión de la seguridad y privacidad de la información (SPI) acorde con los requerimientos institucionales y recursos dispuestos por el Ministerio.

2. ALCANCE

La Gestión de Seguridad y Privacidad de la Información aplica a todos los procesos institucionales. Inicia con la definición del Plan Anual de Seguridad y Privacidad de la Información, continua con su ejecución y finaliza con la evaluación de la gestión.

3. DEFINICIONES Y SIGLAS

ACCIÓN DE MEJORA: Acción permanente realizada con el fin de aumentar la capacidad para cumplir los requisitos y optimizar el desempeño. Es hacer algo mejor de lo que se está haciendo actualmente.
ACCIÓN CORRECTIVA: Conjunto de acciones realizadas para eliminar la(s) causa(s) de una no conformidad detectada u otra situación no deseable, puede existir más de una causa para una no conformidad. La acción correctiva se toma para prevenir que algo vuelva a producirse, mientras que la acción preventiva se toma para prevenir que algo suceda.
ACCIÓN PREVENTIVA: Conjunto de acciones tomadas para eliminar la(s) causa(s) de una no conformidad potencial u otra situación potencialmente indeseable. Puede haber más de una causa para una no conformidad potencial. La acción preventiva se toma para prevenir que algo suceda, mientras que la acción correctiva para prevenir que vuelva a producirse.
ALTA DIRECCIÓN: Persona o grupo de personas que dirigen o controlan una organización al más alto nivel. Definición tomada de la Norma Técnica Colombiana NTC-ISO9000:2000, Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) 2000/12/15.
DOCUMENTO DE DIAGNÓSTICO: Documento que presenta la descripción detallada de la situación problemática, así como los aspectos o factores estratégicos sobre los cuales se debe trabajar en la fase de formulación de la política para dar solución al problema identificado. Fuente: Alcaldía Mayor de Bogotá, Secretaria de Planeación (2017) Guía para la formulación e implementación de políticas públicas del Distrito. ISBN: 978-958-8964-31-7.
GESTIÓN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN: La gestión en Seguridad y Privacidad de la Información en el MinCIT, permite la alineación de la gestión de TI - tecnologías de la información - con los objetivos estratégicos de la entidad; aumenta la eficiencia de la organización y mejora la forma como se prestan los servicios, facilita la administración y el control de los recursos de información y de tecnologías de información que apoyan a los procesos para alcanzar una mayor eficiencia y transparencia en su ejecución así como producción de la información objetiva y oportuna para la toma de decisiones en todos los niveles de la organización.
MESA DE AYUDA: Herramienta virtual que permite el registro, asignación y cierre de solicitudes de soporte técnico mediante el uso de tickets asignados a cada requerimiento. CENTRO DE ATENCIÓN AL USUARIO - HELP DESK ITIL V3 (Operación del Servicio). Punto de contacto para Usuarios para registrar Incidentes, está normalmente más técnicamente focalizado que un Centro de Servicio al Usuario y no proporciona un Punto Único de Contacto. El término Centro de Atención al Usuario es a menudo usado como sinónimo del Centro de Servicio al Usuario.
PLAN: Diseño o esquema detallado de lo que habrá de hacerse a corto, mediano o largo plazo. Deben contener al menos un mínimo acciones, responsables, fechas, resultados esperados y recursos asociados (Colciencias, 2017).

4. GENERALIDADES

4.1 Gestión de la Seguridad y Privacidad de la Información

La Alta Dirección promueve la Seguridad y Privacidad de la Información (SPI), a través del cumplimiento de las políticas de seguridad, privacidad y protección de datos, normatividad y regulación pertinente, la evaluación de activos de información, la valoración y tratamiento de riesgos, la toma de conciencia a través de la Estrategia de Capacitación, Comunicación y Sensibilización, la articulación de los procesos institucionales, la evaluación de la gestión SPI mediante la evaluación interna, el análisis SPI acorde con el instrumento de evaluación MSPI de MinTIC para determinar cambios en la SPI.

El Manual de Gestión de la Seguridad y Privacidad de la Información orienta la organización de la gestión e implementación, mediante la planificación, operación, mantenimiento y mejora de la Seguridad y Privacidad de la Información en el Ministerio.

4.1.1. Plan de Seguridad y Privacidad de la Información

La Oficina de Sistemas de Información como Líder de la Seguridad y Privacidad de la Información (SPI), define anualmente el Plan de Seguridad y Privacidad de la Información (PSPI) conformado por las siguientes líneas de acción y actividades:

4.1.2. Evaluación de la Seguridad y Privacidad de la Información

La Gestión de la Seguridad y Privacidad de la Información se presenta periódicamente en:

4.1.3. RNBD - Registro Nacional de Bases de Datos Personales

En cumplimiento de la Ley 1581 de 2012 que establece los lineamientos para la protección de datos personales, reglamentada mediante Decreto 1377 de 2013 que dicta disposiciones generales para la protección de datos personales y Decreto 886 DE 2014 que reglamenta la información mínima que debe contener el Registro Nacional de Bases de Datos, y a nivel institucional la Resolución MinCIT 2176 de 2016 que adopta el Manual de Políticas Tratamiento de Datos Personales:

a) Acceso a RNBD - Registro Nacional de Bases de Datos
- Acceso al Servicio Web RNBD a través del sitio web www.sic.gov.co de la SIC - Superintendencia de Industria y Comercio.
- El Ministerio en RNBD se autentica con el usuario y contraseña definidos.
b) Registro en RNBD de las Bases con Datos personales
i. El registro de bases de datos o actualización se realiza como mínimo una vez al año, teniendo como base el inventario de bases caracterizadas.
ii. El registro de PQRS y de Incidentes se realiza dos veces al año, con corte a 30 de junio y 31
c) Constancias o Reporte RNBD
Una vez realizado los diferentes registros, RNBD genera la constancia de registro o actualización de bases de datos, y reporte de PQRS o Incidentes registrados.
d) Consulta en RNBD de las Bases con Datos personales
La consulta de las bases de datos registradas en RNBD se realiza con NIT. 960115297 o Razón Social MINISTERIO DE COMERCIO INDUSTRIA Y TURISMO.

4.1.4. Seguridad Digital del SCIT

El Programa de Seguridad Digital del SCIT - Sector Comercio, Industria y Turismo, se centra en dos entornos:
- Mesa de Infraestructura Crítica Cibernética - ICC coordinada por el CCOCI - Comando Conjunto Cibernético de Mindefensa.
- Mesa de Trabajo SCIT coordinada por la Oficina de Sistemas de Información.
El Programa detalla las actividades de articulación y seguimiento transversal relacionado con los compromisos de Seguridad Digital.

4.1.5. Normograma

La normatividad y regulación interna que aplica para la Gestión de la Seguridad y Privacidad de la Información se encuentra disponible para consulta en el Normograma de Seguridad y Privacidad de la Información publicado en la Caracterización del Proceso Sistemas de Gestión.

4.1.6. Roles y Responsabilidades

RESPONSABILIDADES	R		Responsible	Responsable / Encargado	Quien efectivamente realiza la actividad
	A		Accountable	Aprobador	Quien es responsable de que la actividad se realice y rende cuentas sobre su ejecución.
	C		Consulted	Consultado	Quien posee la información o capacidad para realizar la actividad.
	I		Informed	Informado	Quien debe ser informado sobre el avance y los resultados de la ejecución de la actividad.

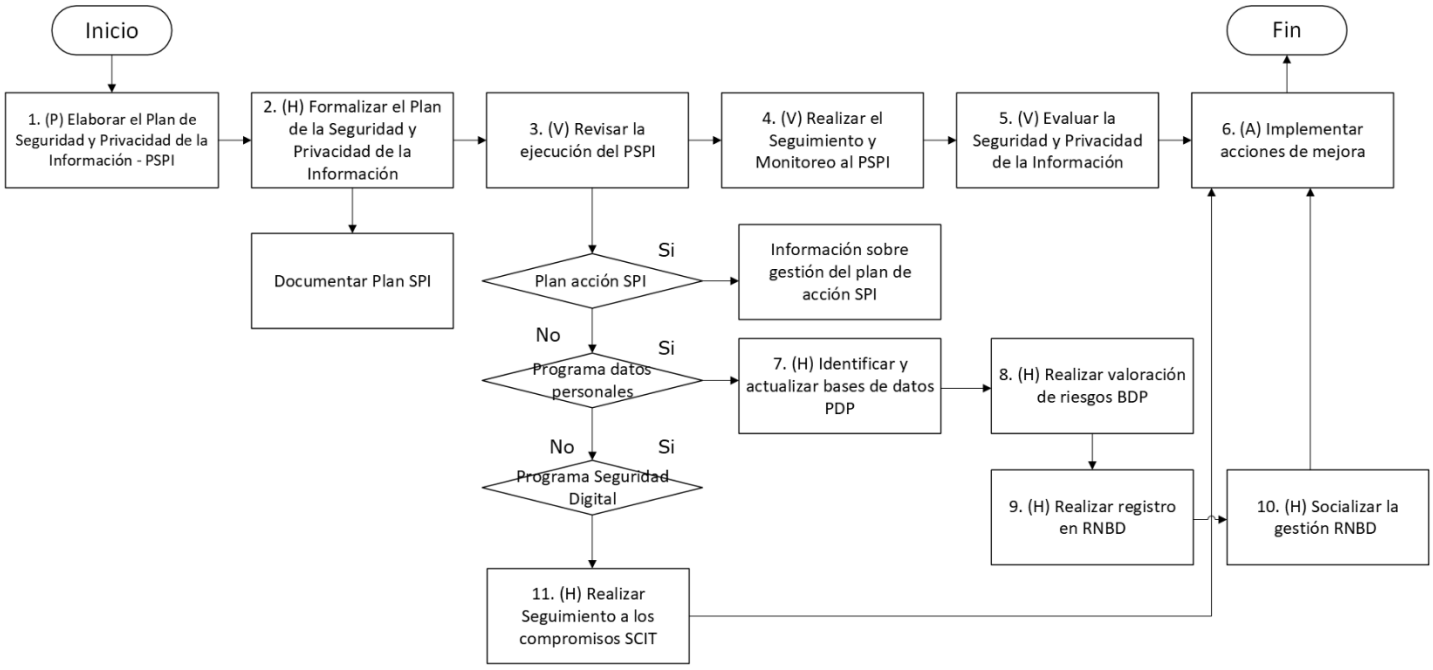
	ROLES	Jefe Oficina Sistemas de Información				Profesional Especializado				Comité Institucional de Gestión y Desempeño				Jefes de Áreas				Entidades SCIT			
	ACTIVIDADES	R	A	C	I	R	A	C	I	R	A	C	I	R	A	C	I	R	A	C	I
1	(P) Elaborar el Plan de Seguridad y Privacidad de la Información - PSPI.	■				■			■												
2	(H) Formalizar el Plan de la Seguridad y Privacidad de la Información.	■				■					■		■								
3	(V) Revisar la ejecución de los programa del PSPI.	■			■	■															
4	(H) Realizar el Seguimiento y Monitoreo al PSPI.	■			■	■															
5	(V) Evaluación de la Seguridad y Privacidad de la Información	■			■	■					■		■								
6	(A) Implementar acciones de mejora.	■			■	■								■	■	■	■				
7	(H) Identificar y actualizar bases de datos PDP	■			■	■								■			■				
8	(H) Realizar valoración de riesgos BDP	■			■	■								■	■	■	■				
9	(H) Realizar registro en RNBD	■			■	■							■								
10	(H) Socialización del registro RNBD	■				■							■								
11	(H) Realizar Seguimiento a los compromisos SCIT	■				■							■							■	■

4.2 Riesgos

- Los riesgos del proceso se encuentran documentados en la matriz de riesgos institucionales.
- Los controles aplicables a cada riesgo se relacionan en las actividades descritas en los documentos y se identifican por medio del código del control.

5. DIAGRAMA DE FLUJO

(A continuación se visualiza de manera gráfica y secuencial las actividades descritas en el numeral 6)



6. DESCRIPCIÓN DE ACTIVIDADES

(A continuación se detallan las actividades graficadas en el numeral 5)

No.	ACTIVIDAD	RESPONSABLE(S)	DESCRIPCIÓN	EVIDENCIA
PSPI - Plan de Seguridad y Privacidad de la Información				
1	(P) Elaborar el Plan de Seguridad y Privacidad de la Información - PSPI	Jefe Oficina de Sistemas de Información	Elaborar el PSPI - Plan de Seguridad y Privacidad de la Información: i. deberá alinearse con los compromisos en la Planeación Estratégica, asociados con la gestión de seguridad y privacidad de la información, ii. deberá determinar los cambios del entorno y normativos relacionados con la seguridad y privacidad de la información. iii. deberá detallar las actividades del plan de acción para el desarrollo, implementación, seguimiento, monitoreo y evaluación de la gestión de seguridad y privacidad de la información, acorde con los indicadores documentados del "Manual de Gestión de Seguridad y Privacidad de la Información". iv. deberá incorporar las actividades para la gestión de datos personales relacionadas con: • Documentación estratégica y de operación para la gestión PDP • Registro RNDB: Bases de Datos, PQRS, Incidentes • Evaluación de la gestión PDP v. deberá incorporar las actividades de articulación con las Entidades del Sector Comercio, Industria y Turismo en materia de seguridad digital. **Tiempo:** Anual	Plan SPI

No.	ACTIVIDAD	RESPONSABLE(S)	DESCRIPCIÓN	EVIDENCIA
2	(H) Formalizar el Plan de la Seguridad y Privacidad de la Información	Jefe Oficina de Sistemas de Información, Profesional Especializado	Presentar al Comité Institucional de Gestión y Desempeño el Plan de la Seguridad y Privacidad de la Información, informando su conformación y alcance: - El plan de acción (operación) SPI - El programa de gestión de datos personales - El programa de seguridad digital Presentar al Comité Institucional de Gestión y Desempeño el seguimiento periódico de la ejecución del Plan de la Seguridad y Privacidad de la Información, precisando: - Documentación estratégica y de operación requerida para la gestión - Registro en RNBD de la información de bases que contengan datos personales - Articulación de las Entidades del Sector para la seguridad digital **Tiempo:** Periódico	GD-FM-001 Acta (comité)
3	(V) Revisar la ejecución del PSPI	Jefe Oficina de Sistemas de Información, Profesional Especializado	Realizar revisiones periódicas de: I. Plan de Acción (operación) SPI Se realiza revisión mensual de las actividades adelantadas en desarrollo de la gestión de activos, riesgos, estrategia de capacitación, comunicación y sensibilización, articulación entre procesos, documentación de la gestión y demás temas relacionados con la gestión de la seguridad y privacidad de la información. II. Programa de Gestión de Datos Personales Se realiza revisión de las actividades adelantadas en desarrollo de la gestión sobre el registro de la información de actualización de las bases de datos en RNBD. Continuar en la actividad 7. III. Programa de Seguridad digital Se realiza revisión de las actividades adelantadas entre el Sector y Entidades de gestión cibernética encargadas de Infraestructuras Críticas y Seguridad Digital del Estado. Continuar en la actividad 11. **Tiempo:** Permanente	TE-FM-017 Inventario de Activos de Información MINCIT /GD-FM-003 Informe
4	(V) Realizar el Seguimiento y Monitoreo al PSPI	Jefe Oficina de Sistemas de Información, Profesional Especializado	Registrar el avance del PSPI en los sistemas ER+ y MIO: I. Seguimiento de la gestión del Plan SPI en el aplicativo ER+ Evaluación por Resultados Realizar para el indicador "Porcentaje de implementación del Plan de Seguridad y Privacidad de la Información" el registro del avance mensual del plan con los soportes respectivos. II. Seguimiento de la Gestión SPI con base en el aplicativo del Modelo Institucional de Operación MIO. Realizar para el indicador "Plan para la Gestión de la Seguridad de la Información" el registro del avance semestral del plan con los soportes respectivos. III. Seguimiento a los indicadores de la Gestión SPI (TE-DR-008 "Manual del Sistema de Gestión de Seguridad y Privacidad de la Información") Realizar el informe de avance de los indicadores de la Gestión SPI para su presentación en el Comité Institucional de Gestión y Desempeño **Tiempo:** Permanente	GD-FM-003 Informe

No.	ACTIVIDAD	RESPONSABLE(S)	DESCRIPCIÓN	EVIDENCIA
5	(V) Evaluar la Seguridad y Privacidad de la Información	Jefe Oficina de Sistemas de Información, Profesional Especializado	Evaluar la gestión SPI conforme al procedimiento de auditoría vigente y bajo el estándar ISO/IEC 27001, de acuerdo con la programación definida por la Oficina Asesora de Planeación Sectorial. **Tiempo:** Permanente	GD-FM-001 Acta (Comité)
6	(A) Implementar acciones de mejora	Jefe Oficina de Sistemas de Información, Profesional Especializado	Implementar las acciones de mejora y se documentará su gestión según la programación definida para cada acción en el aplicativo correspondiente - Acciones de Mejora. **Tiempo:** Permanente	Aplicativo vigente
Programa para la Gestión de Datos Personales				
7	(H) Identificar y actualizar bases de datos PDP	Jefe Oficina de Sistemas de Información, Profesional Especializado, Jefe(s) de Oficina	Identificar y actualizar anualmente las bases de datos personales (BDP) en coordinación con las áreas: I. Identificar y actualizar BDP - Bases con Datos Personales Como mínimo una vez al año se adelanta en coordinación con las áreas la documentación de nuevas bases y actualización de las inventariadas anteriormente. Se aplica el formato " Caracterización BDP". II. Revisar caracterizaciones: En la revisión de las Caracterizaciones se tiene en cuenta aspectos como: tipo de base de datos, responsables y/o encargados, titulares, PQRS, transferencia y transmisión de datos, entre otros criterios. Ir a actividad 8, para realizar el análisis de riesgos a bases con datos personales III. Consolidar un inventario de bases con datos personales para realizar registros. **Tiempo:** Permanente	TE-FM-018 Caracterización BDP
8	(H) Realizar valoración de riesgos BDP	Profesional Especializado, Jefe(s) de Oficina, Jefe Oficina de Sistemas de Información	Realizar análisis y valoración de riesgo atendiendo el lineamiento definido en el documento "Política y Metodología para la Administración de Riesgos y Oportunidades". Documentar los riesgos en el formato "Matriz de Riesgos" Establecer acciones de tratamiento conforme a la metodología del documento "Política y Metodología para la Administración de Riesgos y Oportunidades" y de acuerdo con el cronograma establecido: • Se realiza el seguimiento periódico de las acciones de tratamiento con los encargados • Se documentan las acciones en la herramienta definida para su trazabilidad. **Tiempo:** Permanente	TE-FM-019 Matriz Riesgos de seguridad y privacidad de la información
9	(H) Realizar registro en RNBD	Jefe De Oficina, Jefe Oficina de Sistemas de Información, Profesional Especializado	Registrar y actualizar la información de las bases de datos personales, PQRS e incidentes en el RNBD, a partir de las caracterizaciones realizadas. **Tiempo:** Permanente	Reporte RNBD
10	(H) Socializar la gestión RNBD	Jefe Oficina de Sistemas de Información, Profesional Especializado	Publicar en el sitio web institucional los registros RNBD y solicitar su publicación al Grupo de Comunicaciones en el sitio de Transparencia y Acceso a la Información. **Tiempo:** Permanente	GD-FM-003 Informe

No.	ACTIVIDAD	RESPONSABLE(S)	DESCRIPCIÓN	EVIDENCIA
Programa Seguridad Digital SCIT				
11	(H) Realizar Seguimiento a los compromisos SCIT	Jefe Oficina de Sistemas de Información, Profesional Especializado	Realizar seguimiento a los compromisos adquiridos en la Mesa de Infraestructura Crítica Cibernética (ICC) y en la Mesa de Seguridad Digital del Sector, se realiza seguimiento periódico a: - Mesa ICC - Participación en la Mesa ICC De acuerdo con la convocatoria del CCOCI - Comando Conjunto Cibernético, se agendará a las Entidades del Sector para su participación y atención a las indicaciones de ciberseguridad para ICCs. - Actualización del Catálogo ICC del Sector Comercio, Industria y Turismo - SCIT Conforme a las indicaciones del CCOCI y la metodología definida se coordina con las Entidades del Sector la actualización y reporte del Catálogo ICC en las fechas indicadas. - Actualización del Planees ICC del SCIT Atendiendo la metodología del CCOCI se revisa los Planees ICC del SCIT para determinar los ajustes de acuerdo con los cambios del entorno de ciberseguridad de las Entidades y efectuar su actualización. . Mesa Seguridad Digital del SCIT - Compromisos FURAG - Seguridad Digital Conforme a la Política de Seguridad Digital, se revisan los compromisos MSPI y de Seguridad Digital implementados por el SCIT. - Planes de Seguridad Digital Seguimiento a las Alertas de los Planes ICC del Sector y avance en el Plan SPI. II. Elaborar Informe de Seguimiento Realizar el informe periódico de seguimiento de los compromisos del Programa de Seguridad Digital del SCIT para informar al Comité Institucional de Gestión y Desempeño. **Tiempo:** Permanente	GD-FM-003 Informe

7. FORMATOS DEL PROCEDIMIENTO

No.	CODIGO	NOMBRE DEL FORMATO
1	GD-FM-001	Acta
2	TE-FM-017	Inventario de Activos de Información MINCIT
3	TE-FM-018	Caracterización BDP
4	TE-FM-019	Matriz Riesgos de seguridad y privacidad de la información
5	GD-FM-003	Informe

8. HISTORIAL DE CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO
12/06/2026	0	Primera versión del documento para el nuevo Mapa de procesos. Código anterior: GTI-PR-011.V01. Para efectos de trazabilidad y soporte de la migración al nuevo aplicativo de administración de la documentación del Modelo Institucional de Operación (MIO), los siguientes fueron los responsables de la revisión y aprobación del documento migrado: REVISÓ: MARIA DEL ROSARIO CHACÓN HERRERA – Cargo: Profesional especializado OSI APROBÓ: EDGAR GREGORIO CARRILLO MONCADA – Cargo: Jefe OSI Desde la OAPS se asegura que el contenido corresponde a la última versión vigente en ISOlución al momento de la migración a MIOsoft.

9. FLUJO DE APROBACIÓN

ELABORÓ		APOYO OAPS		REVISÓ		APROBÓ	
Nombre:		Nombre:	Jefferson López Saavedra	Nombre:		Nombre:	
Cargo:		Cargo:	Profesional Especializado	Cargo:		Cargo:	