Manual

Privacidad y seguridad de la información

Unidad de Proyección Normativa
y Estudios de Regulación
Financiera - **URF**

Contenido

1. Introducción

El Modelo Integrado de Planeación y Gestión- MIPG contempla las políticas seguridad y gobierno digital, que se desarrollan en el marco de la estrategia de gobierno digital en adelante EDG. La EGD pretende transformar a las entidades públicas y dotarlas de capacidades que les permitan responder a las necesidades que demanda un escenario de economía digital y establecer ciudades y territorios inteligentes que les ofrezcan mejores condiciones a los ciudadanos y un nivel superior de vida, a partir de la perspectiva TIC para el Estado y TIC para la sociedad. La política de gobierno digital es transversal a todas las políticas de MIPG, puesto que es soporte para apalancarlas a través de un estado que presta bienes y servicios soportado en el uso de las TIC.

En este sentido, mediante el Decreto 1075 de 2015, se definió el componente de privacidad y seguridad de la información, como un componente integral de la estrategia de gobierno digital. En desarrollo de este componente, MinTIC elaboró un manual con el modelo de seguridad y privacidad de la información - MPSI, que contempla buenas prácticas de seguridad de la información, lineamientos de transparencia y acceso a la información pública y un marco de arquitectura TI, operativo a partir de cinco (5) fases y seis (6) niveles de madurez que corresponden a la evolución de la implementación del modelo.

El MPSI establece que es fundamental implementar controles para la gestión de los riesgos, partiendo de una valoración del nivel de criticidad, para implementar la protección debida, con el fin de mitigar y/o evitar posible pérdida de su disponibilidad, integridad y confidencialidad. Lo anterior, teniendo en cuenta el aumento de los incidentes de seguridad de la información en las entidades, los cuales generan pérdidas financieras, de imagen, de información, datos y la generación de reprocesos administrativos. Por lo tanto, es necesario implementar, mantener y mejorar de manera continua la gestión de la privacidad y seguridad de la información, mediante el diseño, documentación, implementación y monitoreo de controles basados en una gestión de riesgos que minimice el impacto o la probabilidad de ocurrencia, a fin de mantenerlos en niveles aceptables.

En relación con lo expuesto, la Unidad suscribió el convenio de cooperación No. 002 de 2016 con el Ministerio de Hacienda y Crédito Público, que establece en el alcance de su objeto: *"Para la ejecución del presente Convenio EL MINISTERIO prestará apoyo en la gestión administrativa de la URF, que incluye entre otros aspectos, el apoyo en temas de recursos humanos, gestión documental, comunicaciones, tecnológicos, logísticos, de planeación y control interno" […].* Esto con el propósito de dar cumplimiento a los requerimientos relacionados con la privacidad y seguridad de la información, entre otros.

En virtud de la referida colaboración interinstitucional, la Unidad comparte oficinas con el Ministerio de Hacienda y Crédito Público y hace uso de los recursos y aplicaciones tecnológicas de este, en lo relacionado con la página web y los sistemas de información.

En el caso de los recursos tecnológicos, la Dirección de Tecnología del Ministerio opera los servicios y soluciones TIC y la infraestructura que los soportan, incluidos los computadores y el software que utiliza la Unidad, a través de su mesa de ayuda y del centro de servicios tecnológicos. Por lo anterior, el alcance del Plan Estratégico Institucional de las Tecnologías de la Información - PETI del Ministerio de Hacienda y Crédito Público incluye a la Unidad.

En consecuencia, la Unidad de Proyección Normativa y de Estudios de Regulación Financiera – URF, presenta el manual de privacidad y seguridad de la información, que se articula con el MPSI del Ministerio de Hacienda y Crédito Público y que sirve como instrumento para implementar un modelo de gestión de la seguridad de la información basado en la mitigación del riesgo, encaminado a generar cultura en torno al uso adecuado de la información. El manual consolida el alcance, los productos esperados, los procedimientos, la operación y la metodología de gestión de riesgo del MPSI. Esto teniendo en cuenta que la información es un activo de suma importancia, toda vez que es indispensable para la toma de decisiones, la garantía de derechos fundamentales y el cumplimiento de los fines esenciales del Estado.

2. Objetivo

Definir las estrategias y mecanismos mediante los cuales se desarrollan e implementan los componentes del modelo de privacidad y seguridad de la información, por medio de su delimitación conceptual y operación, basada en los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones- MinTIC, para garantizar la protección de la información y la privacidad de los datos de los grupos de valor y partes interesadas de la Unidad.

2.1 Objetivos específicos

- Desarrollar los aspectos conceptuales y metodológicos del modelo de privacidad y seguridad de la información
- Establecer roles y responsabilidades para la implementación del modelo de privacidad y seguridad de la información
- Presentar las actividades, periodicidad y herramientas para la implementación del modelo de privacidad y seguridad de la información
- Sensibilizar a los servidores, pasantes, proveedores y grupos de valor y partes interesadas sobre la importancia de la privacidad y seguridad de la información

3. Alcance

Inicia con la definición conceptual del modelo de privacidad y seguridad de la información y finaliza con su evaluación y mejoramiento. Cubre las actividades necesarias para su planificación, implementación y seguimiento.

4. Productos esperados

- Plan de privacidad y seguridad de la información
- Procedimientos de privacidad y seguridad de la información

5. Términos y definiciones

- **Acceso a la información pública:** derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

- **Activo de información:** activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

- **Amenazas**: causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Análisis de riesgo:** proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Datos personales:** cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- **Datos personales públicos**: dato que no es semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

- **Datos personales privados:** dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

- **Datos personales mixtos:** información que contiene datos personales públicos junto con datos privados o sensibles.

- **Datos personales sensibles:** aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

- **Encargado del tratamiento de datos:** persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros realice el tratamiento de datos personales por cuenta del responsable del tratamiento. (Ley 1581 de 2012, art 3).

- **Información pública clasificada:** aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Información pública reservada**: aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Ley de transparencia y acceso a la información pública:** Ley Estatutaria 1712 de 2014.

- **Mecanismos de protección de datos personales:** lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

- **MHCP:** Ministerio de Hacienda y Crédito Público

- **Privacidad:** derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar.

- **Responsable del tratamiento de datos:** persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

- **Riesgo:** posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguridad de la información:** preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **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 organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

- **Titulares de la información:** personas naturales cuyos datos personales sean objeto de tratamiento. (Ley 1581 de 2012, art 3)

- **Tratamiento de datos personales:** cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

- **Trazabilidad:** cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

- **Vulnerabilidad:** debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

6. Roles y responsabilidades

Roles	Responsabilidades
Comité Institucional de Gestión y Desempeño	• Hacer seguimiento a la privacidad y seguridad de la información en la Unidad, a partir de las políticas institucionales de gestión y desempeño • Identificar oportunidades de mejora
Proceso gestión de información	• Diseñar y proponer estrategias para la operación de las directrices establecidas en el manual • Establecer las acciones necesarias para el logro de objetivos • Articular a los actores necesarios durante la ejecución de las actividades y estrategias propuestas
Proceso gestión de comunicaciones	• Apoyar el componente cultural, mediante la construcción y difusión de mensajes relacionados con la importancia de la privacidad y seguridad de la información, previa solicitud del proceso de gestión de la información
Servidores de la URF	• Asumir un rol activo en lo relacionado con la privacidad y seguridad de la información, de conformidad con lo establecido en el manual y la normatividad vigente

7. Desarrollo técnico, conceptual y metodológico del manual

El Modelo Integrado de Planeación y Gestión- MIPG contempla las políticas de gobierno y seguridad digital que se desarrollan en el marco de la estrategia de gobierno digital, que fomenta la transformación de las entidades públicas, dotándolas de capacidades que les permitan responder a las necesidades que demanda un escenario de economía digital, así como al establecimiento y desarrollo de ciudades y territorios inteligentes para ofrecer mejores condiciones a los ciudadanos y un nivel superior de vida. No se trata únicamente de automatizar procesos o de atender la provisión de trámites y servicios para la ciudadanía, sino de empoderarlos, a partir de la perspectiva TIC para la sociedad.

En este sentido, MinTIC , mediante el Decreto 1075 de 2015, definió el componente de privacidad y seguridad de la información, como un componente integral de la estrategia y elaboró un modelo de seguridad y privacidad de la

información, el cual contempla buenas prácticas, lineamientos de transparencia y acceso a la información pública y un marco de arquitectura TI, operativo a partir de cinco (5) fases y seis (6) niveles de madurez que corresponden a la evolución en la implementación del mismo.

A continuación, se presenta gráficamente el ciclo de operación y los niveles de madurez del modelo:

Ilustración 1. Ciclo de operación del modelo de seguridad y privacidad de la información. Fuente MinTIC

Niveles de madurez

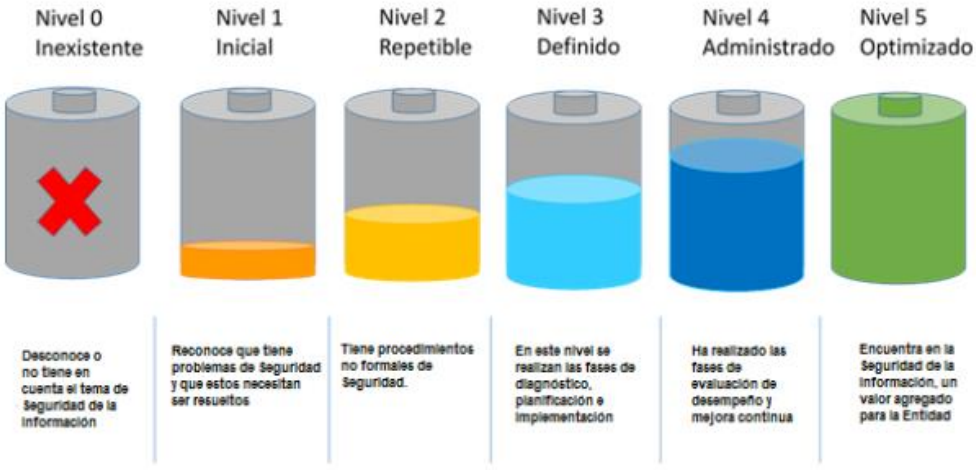

Ilustración 2. Niveles de madurez del modelo. Fuente MinTIC

7.1. Descripción del ciclo de operación

El ciclo de operación del modelo de privacidad y seguridad de la información comprende cinco fases que se complementan:

7.1.1. Fase diagnóstica

Es una de las etapas previas a la implementación, que pretende identificar el estado actual de la entidad con relación a los requerimientos del modelo. Para su ejecución se requiere contar con el autodiagnóstico del modelo (matriz autodiagnóstico MinTIC) y los resultados de las auditorías y fuentes de información primaria. Los pasos para seguir son:

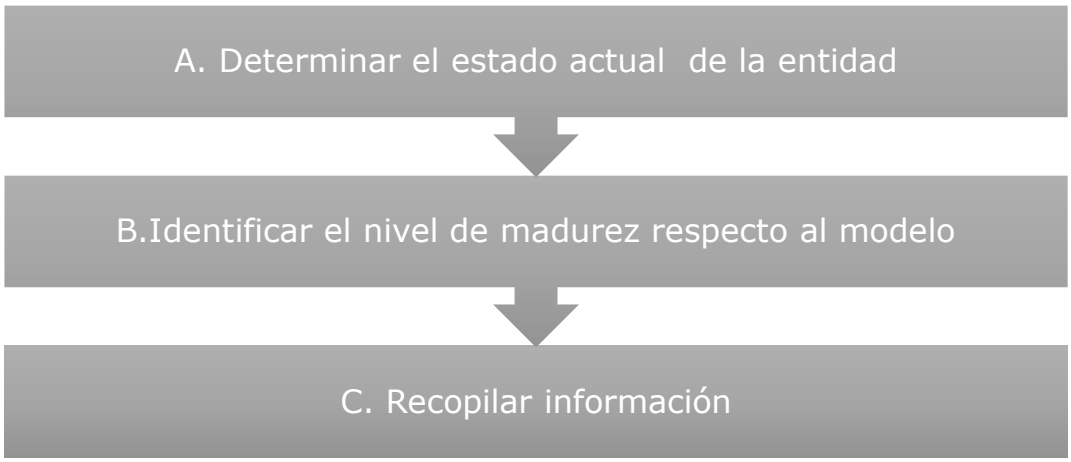

Ilustración 3. Fase diagnóstica. Elaboración propia.

7.1.2. Fase planeación

Con los resultados de la etapa anterior, se elabora el plan de privacidad y seguridad de la información, para definir las estrategias y mecanismos necesarios para la implementación del modelo. Para este fin se debe tener en cuenta:

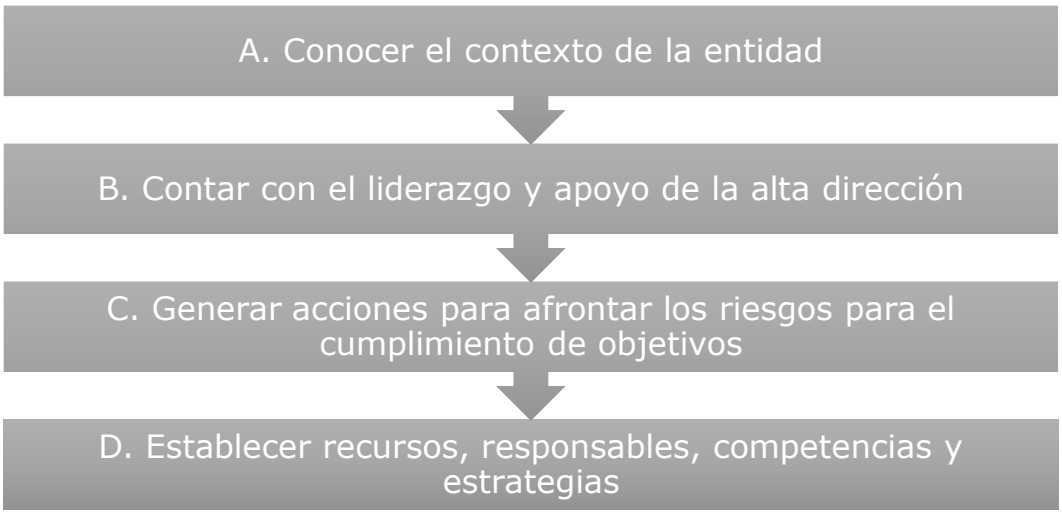

Ilustración 4. Fase planeación. Elaboración propia.

7.1.3. Fase implementación

Esta fase comprende la ejecución de las actividades y estrategias definidas en la etapa de planeación. La Unidad de Proyección Normativa y Estudios de Regulación Financiera define, implementa, evalúa y mejora las estrategias de privacidad y seguridad de la información en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la privacidad y seguridad de la información, con base en el Modelo de Privacidad y Seguridad de la Información -MPSI, así como en la política de riesgos de la entidad donde se integra lo referente a privacidad y seguridad de la información y lo establecido para la gestión de incidentes.

Además, se articula con las políticas, procedimiento, manuales y protocolos del Ministerio de Hacienda y Crédito Público en lo referente a la plataforma tecnológica, para dar cumplimiento al plan de privacidad y seguridad de la información, en virtud de lo establecido en el convenio interadministrativo 002 de 2016 que tiene como objeto *"Para la ejecución del presente Convenio EL MINISTERIO prestará apoyo en la gestión administrativa de la URF, que incluye entre otros aspectos, el apoyo en temas de recursos humanos, gestión documental, comunicaciones, tecnológicos, logísticos, de planeación y control interno"*

Los procedimientos del Ministerio de Hacienda y Crédito Público relacionados con privacidad y seguridad de la información que comprenden en su alcance a la Unidad son:

- Gestión de incidentes
- Gestión demanda estratégica TIC
- Gestión de cambios tecnológicos y liberación TIC
- Procedimiento de continuidad.
- Seguimiento de aplicativos de software.
- Gestión de acceso de usuarios.
- Gestión de garantías de equipos y componentes ubicados en los centros de cómputo
- Gestión de Usuarios Administradores de la plataforma tecnológica (segunda cuenta)
- Gestión de incidentes de seguridad de la información
- Recuperar Contraseña Administrador Local
- Extracción de Información
- Gestión de requerimientos de Servicios TIC
- Mantenimiento de Software
- Respaldo de información en los servidores
- Recuperación de información en los servidores

En consecuencia, para la fase de implementación se deben tener en cuenta los procedimientos del Ministerio de Hacienda y Crédito Público y las siguientes actividades:

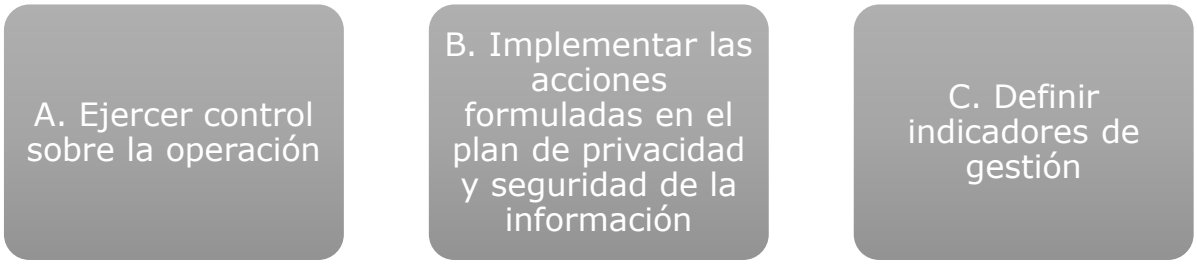

Ilustración 5. Fase implementación. Elaboración propia.

7.1.4. Fase de evaluación

La evaluación y mejora se realiza con base en los resultados de los indicadores propuestos, a fin de validar la eficacia, eficiencia y efectividad de las acciones ejecutadas en el marco del plan de privacidad y seguridad de la información. Para este efecto se debe tener en cuenta:

Ilustración 6. Fase evaluación. Elaboración propia.

7.1.5. Fase de mejora continua

Una vez identificados los resultados de la evaluación, se procede con el diseño de las acciones correctivas a las desviaciones que se evidencien, con el propósito de fortalecer la mejora continua en la aplicación del modelo de privacidad y seguridad de la información. Esto permitirá avanzar constantemente en la gestión de los riesgos, para mantenerlos en un nivel aceptable y enmarcar la gestión en un ciclo de mejora continua, como se presenta en el siguiente esquema:

Ilustración 7. Esquema mejora continua. Elaboración propia.

7.2. Actividades para la implementación del MPSI

Las actividades necesarias para operar el MPSI en la Unidad, comprenden un conjunto de tareas y productos definidos en las fases descritas en el numeral anterior y se detallan en la siguiente tabla:

Componente	Actividad	Descripción	Estrategia o mecanismo	Periodicidad	Producto
Diagnóstico	Diligenciar la herramienta de autodiagnóstico	Diligenciar el autodiagnóstico para identificar el nivel de madurez de la entidad frente a la privacidad y seguridad de la información y así determinar su estado actual	Reunión con líderes de procesos institucionales/ mesa técnica	Revisión anual o cuando sea requerido	Plan de privacidad y seguridad de la información
	Elaborar política de seguridad y privacidad de la información	Elaborar documento que define el compromiso institucional respecto a la aplicación de un modelo de privacidad y seguridad de la información, debidamente aprobado por la alta dirección	Elaboración de la política de seguridad y privacidad de la información	Revisión anual o cuando sea requerido	Política de seguridad y privacidad de la información
	Elaborar procedimientos de privacidad y seguridad de la información	Elaborar documentación de los procedimientos que desarrollan la operación del modelo de privacidad y seguridad de la información	Alineación de la operación con los procedimientos del Ministerio de Hacienda y Crédito Público (Convenio 002 de 2015)	Revisión anual o cuando sea requerido	Procedimientos de privacidad y seguridad de la información
	Elaborar o actualizar los inventarios de activos de información	Elaborar documento con la metodología y la caracterización de los activos de información que contengan datos personales	Reuniones de trabajo con los productores de la información	Revisión anual o cuando sea requerido	Inventario de activos de información

Por responsabilidad ambiental no imprima este documento - Las copias impresas o guardadas fuera del SMGI, se consideran "Copias no Controladas"; la versión vigente está disponible en el módulo de documentos del SMGI.
GI-FT-021_V3 - Documento referente: Manual de producción y administración de documentos

Componente	Actividad	Descripción	Estrategia o mecanismo	Periodicidad	Producto
Planeación	Integrar el modelo de privacidad y seguridad de la información con el sistema de gestión institucional - SGI	Realizar la integración del MPSI con el SGI	Reuniones de trabajo con los operadores del SGI	Revisión anual o cuando sea requerido	MPSI integrado al SGI
	Identificar y valorar los riesgos de privacidad y seguridad de la información	Elaborar documento con la metodología de gestión de riesgos	Reuniones de trabajo con el profesional de direccionamiento y planeación	Revisión anual o cuando sea requerido	Riesgos identificados y valorados
	Definir indicadores de gestión	Elaborar documento con la descripción de los indicadores de gestión	Reuniones de trabajo con el profesional de direccionamiento y planeación	Cuando sea requerido	
	Estrategia de comunicación	Definir la estrategia para comunicar la parte estratégica del modelo de privacidad y seguridad de la información	Reuniones de trabajo con el profesional de gestión de comunicaciones	Anual	Modelo socializado en la Unidad

Por responsabilidad ambiental no imprima este documento - Las copias impresas o guardadas fuera del SMGI, se consideran "Copias no Controladas"; la versión vigente está disponible en el módulo de documentos del SMGI.
GI-FT-021_V3 - Documento referente: Manual de producción y administración de documentos

Componente	Actividad	Descripción	Estrategia o mecanismo	Periodicidad	Producto
Implementación	Ejercer control sobre la operación	Adelantar el control sobre la operación del MPSI	Adelantar control sobre la operación	Cuatrimestral o cuando sea requerido	Operación controlada
	Implementar acciones formuladas en el plan de privacidad y seguridad de la información	Realizar informe de la ejecución del plan de privacidad y seguridad de la información	Implementar acciones	Anual	Informe de ejecución del plan de privacidad y seguridad de la información
Evaluación	Elaborar plan de seguimiento y revisión del MPSI	Elaborar plan de seguimiento y revisión del MPSI y someterlo a revisión de la alta dirección	Reuniones de trabajo con el profesional de direccionamiento y planeación	Anual	Plan de seguimiento y revisión del MPSI
	Ejecutar el plan de seguimiento y evaluación del MPSI	Adelantar el seguimiento y evaluación del MPSI	Ejecutar plan de seguimiento y evaluación	Anual	Informe de seguimiento y evaluación del MPSI
Mejora continua	Socializar los resultados y adelantar acciones de mejora	Socializar los resultados con la alta dirección, en el Comité Institucional de Gestión y Desempeño y acordar acciones para la mejora continua	Campañas de sensibilización	Anual	Acta del Comité

Por responsabilidad ambiental no imprima este documento - Las copias impresas o guardadas fuera del SMGI, se consideran "Copias no Controladas"; la versión vigente está disponible en el módulo de documentos del SMGI.
GI-FT-021_V3 - Documento referente: Manual de producción y administración de documentos

Los productos definidos en el cuadro anterior se reflejan en los documentos asociados al proceso de gestión de la información, instrumentos de información pública y demás herramientas necesarias para su desarrollo. La revisión del estado de los productos se realiza de forma anual y de ser necesario se incluyen acciones en el plan de acción de cada vigencia.

8. Documento referente

Tipo	Nombre
Política	Política de privacidad y seguridad de la información

9. Datos de elaboración y control de cambios

Control de cambios			
Fecha	**Versión**	**Cód. Solicitud**	**Descripción del cambio**
2023-08-10	1	TS-0306	Elaboración del documento.

Elaboración, revisión y aprobación	
Elaboración	
Nombre:	Juan Stiven Ríos Andrade
Cargo:	Profesional especializado
Revisión	
Nombre:	Daissy Tatiana Santos Yate
Cargo:	Profesional especializado
Aprobación	
Nombre:	Ivonnie Edith Gallardo Gómez
Cargo:	Subdirectora Jurídica y de Gestión Institucional

Por responsabilidad ambiental no imprima este documento - Las copias impresas o guardadas fuera del SMGI, se consideran "Copias no Controladas"; la versión vigente está disponible en el módulo de documentos del SMGI.
GI-FT-021_V3 - Documento referente: Manual de producción y administración de documentos