



Manual

Privacidad y seguridad de la información



Unidad de Proyección Normativa
y Estudios de Regulación Financiera



Contenido

1.	Introducción	2
2.	Objetivo	3
3.	Alcance	3
4.	Productos esperados	3
5.	Términos y definiciones	4
6.	Roles y responsabilidades	7
7.	Desarrollo técnico, conceptual y metodológico del manual.....	8
7.1	Descripción del ciclo de operación	9
7.1.1	Fase diagnóstica	10
7.1.2	Fase planeación	10
7.1.3	Fase implementación.....	11
7.1.4	Fase de evaluación.....	12
7.1.5	Fase de mejora continua	13
7.2	Gestión de activos de información	13
7.3	Actividades para la implementación del MPSI.....	14
8.	Documento referente	19
9.	Datos de elaboración y control de cambios.....	19

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.

A través del Decreto 1075 de 2015, se estableció la privacidad y seguridad de la información como parte fundamental de la estrategia de gobierno digital. Para impulsar este componente, MinTIC creó un manual que describe el modelo de seguridad y privacidad de la información (MPSI). Este modelo incluye buenas prácticas de seguridad, pautas de transparencia y acceso a la información pública, así como una arquitectura tecnológica dividida en cinco fases y seis niveles de madurez, los cuales reflejan el progreso en 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.

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 lo siguiente: "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.

Mediante el presente documento la URF presenta el manual de privacidad y seguridad de la información, alineado con el MPSI del Ministerio de Hacienda. Este manual facilita la gestión de la seguridad de la información mediante la mitigación del riesgo y promueve el uso responsable de los datos. Define alcance, productos, procedimientos, operación y métodos de gestión de riesgos, reconociendo la información como un activo fundamental para la toma de decisiones, la protección de derechos y el cumplimiento de los fines estatales.

2. Objetivo

Desarrollar las estrategias y mecanismos mediante los cuales se 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, incorporando la gestión de riesgos, para asegurar la confidencialidad, integridad y disponibilidad de la información, la continuidad del negocio, así como la protección de la información y la privacidad de los datos de los grupos de valor y partes interesadas de la Unidad.

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.

Asimismo, el presente manual aplica a todos los activos de información de la Entidad, incluyendo información física y digital, sistemas de información, infraestructura tecnológica, procesos institucionales, así como a todos los funcionarios, contratistas, terceros y proveedores que accedan, gestionen o administren información, incluyendo los entornos de trabajo remoto o teletrabajo.

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).
- **Control:** Medida administrativa, técnica o física implementada para gestionar riesgos.
- **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, compilado en el Decreto 1074 de 2015).
- **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, compilado en el Decreto 1074 de 2015).
- **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).
- **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 de seguridad digital:** Es la combinación de amenazas y/o vulnerabilidades que se pueden materializar en el curso de cualquier actividad en el entorno digital y que puede afectar el logro de los objetivos económicos o sociales al alterar la confidencialidad, integridad y disponibilidad.
- **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	Línea de defensa a la que pertenece el rol	Responsabilidades
Comité Institucional de Gestión y Desempeño	Línea estratégica	<ul style="list-style-type: none"> Hacer seguimiento al modelo de privacidad y seguridad de la información de la Unidad, Identificar oportunidades de mejora para fortalecer la gestión y el desempeño institucional en materia de PSI. Aprobar las estrategias diseñadas para la operación de las directrices establecidas en el manual, orientadas al fortalecimiento de la gestión y el desempeño institucional en materia de PSI.
Proceso gestión de información	Segunda línea	<ul style="list-style-type: none"> 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	Tercera línea	<ul style="list-style-type: none"> 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	Primera línea	<ul style="list-style-type: none"> 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
Proceso de control y evaluación	Tercera línea	<ul style="list-style-type: none"> Realizar evaluación independiente sobre la gestión de seguridad de la información en la Unidad

Todos los roles definidos en la Entidad deberán asumir responsabilidades relacionadas con la identificación, gestión y tratamiento de los riesgos de seguridad de la información, el reporte oportuno de incidentes de seguridad, así como el cumplimiento de las políticas, lineamientos y controles asociados a estos.

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

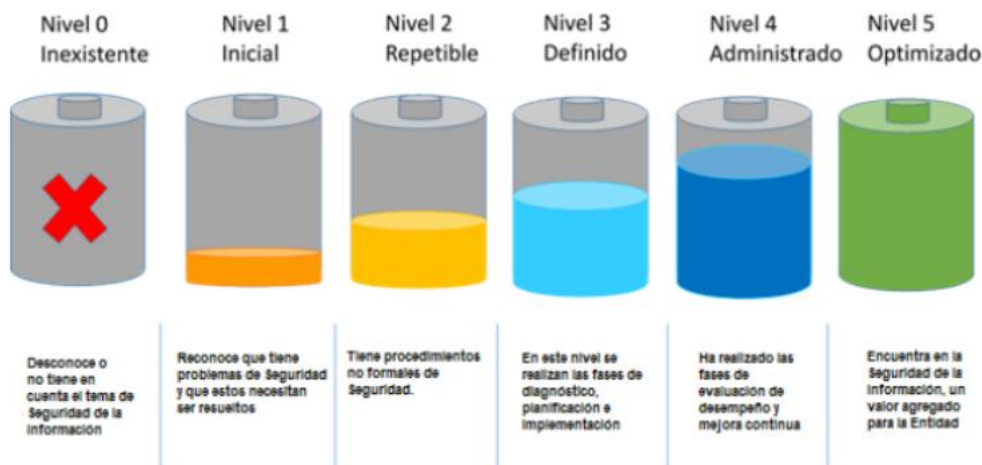


Ilustración 2. Niveles de madurez del modelo. Fuente MinTIC

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 a seguir son:

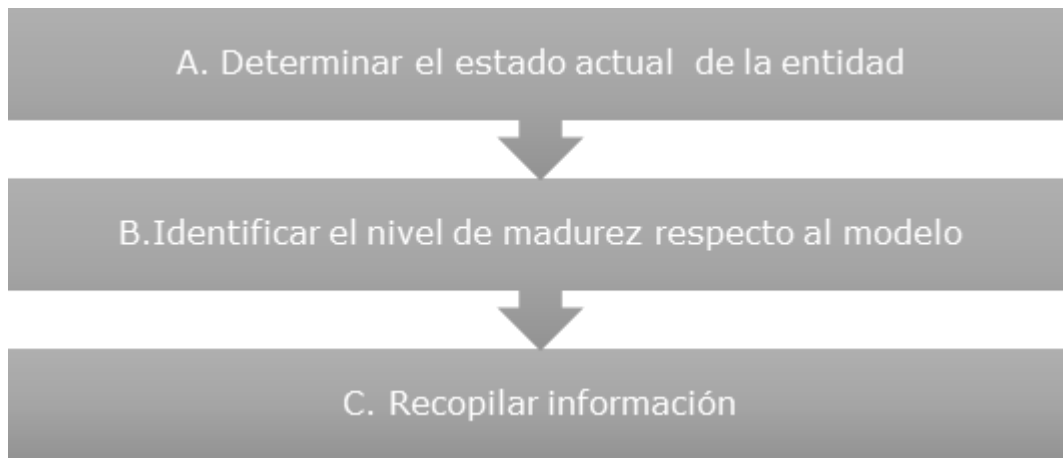


Ilustración 3. Fase diagnóstica. Elaboración propia.

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:

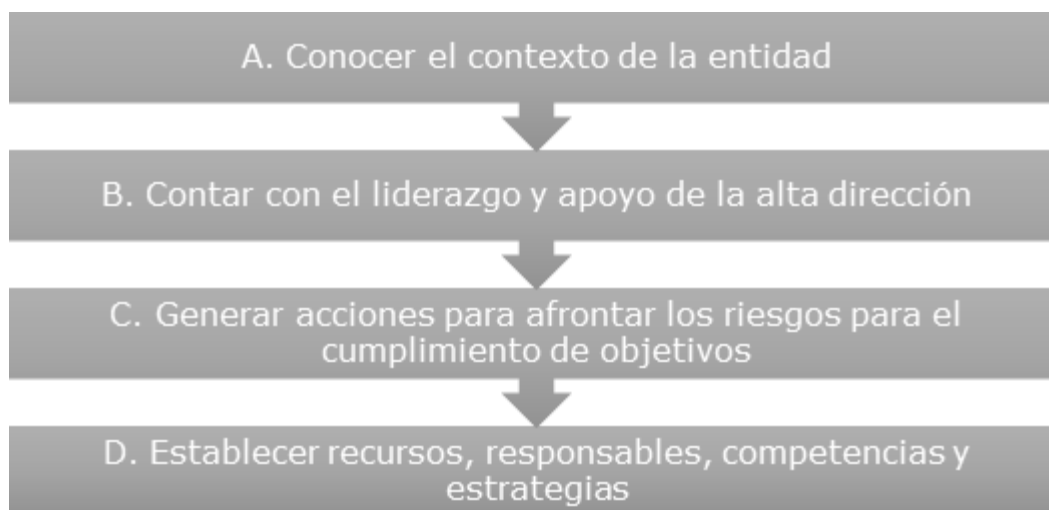


Ilustración 4. Fase planeación. Elaboración propia.

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 el siguiente: *"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:

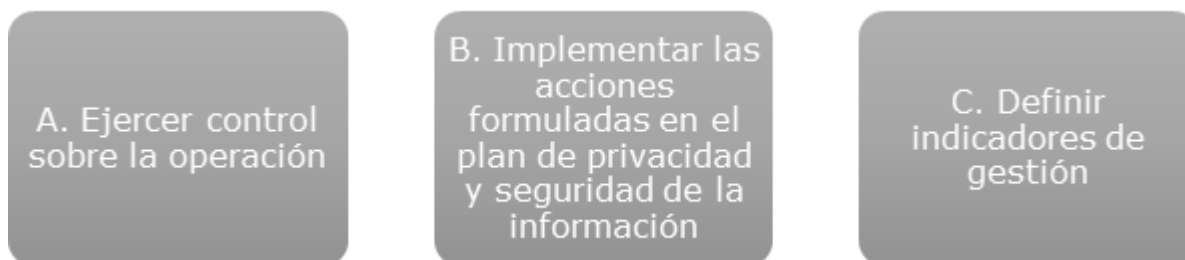


Ilustración 5. Fase implementación. Elaboración propia.

7.1.4 Fase de evaluación

La evaluación y mejora se realiza 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.

El monitoreo y evaluación del modelo de privacidad y seguridad de la información se realizará mediante el monitoreo de riesgos y la revisión de los planes de mejoramiento, en articulación con el Sistema de Gestión Institucional.

El proceso de Control y Evaluación verificará periódicamente el cumplimiento de los lineamientos establecidos, generando recomendaciones orientadas a la mejora continua.

7.1.5 Fase de mejora continua

Una vez identificados los resultados de la evaluación, se procede con la revisión de los planes de mejoramiento y validación de 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 Gestión de activos de información

La Unidad establecerá y mantendrá un inventario actualizado de activos de información, el cual incluirá su identificación, clasificación, ubicación, responsable y nivel de criticidad.



Los activos de información serán clasificados de acuerdo con su nivel de sensibilidad (pública, clasificada o reservada), con el fin de definir los controles de seguridad adecuados para su protección.

Cada activo deberá contar con un responsable encargado de su adecuado uso, protección y actualización.

7.3 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
	Analizar resultados del autodiagnóstico	Analizar los resultados obtenidos en el autodiagnóstico con el fin de identificar brechas, oportunidades de mejora y el nivel de madurez de la entidad en materia de privacidad y seguridad de la información.	Mesas de trabajo con líderes de proceso y revisión técnica de los resultados obtenidos en la herramienta de autodiagnóstico.	Anual o cuando se realice el autodiagnóstico	Informe de resultados del autodiagnóstico
	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 el Comité de Gestión y Desempeño Institucional.	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



Componente	Actividad	Descripción	Estrategia o mecanismo	Periodicidad	Producto
Planeación	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
	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 el proceso de direccionamiento y planeación	Revisión anual o cuando sea requerido	MPSI integrado al SGI
	Identificar y valorar los riesgos de privacidad y seguridad de la información	Identificar y valorar los riesgos de privacidad y seguridad de la información, con el fin de definir acciones de control y mitigación que protejan la información institucional.	Reuniones de trabajo con los responsables de activos de información	Revisión anual o cuando sea requerido	Riesgos identificados y valorados
	Definir indicadores de gestión	Formular y mantener el indicador de cumplimiento del plan de privacidad y seguridad de la información.	Reuniones de trabajo con el profesional de direccionamiento y planeación	Cuando sea requerido	Indicadores de gestión definidos y documentados



Componente	Actividad	Descripción	Estrategia o mecanismo	Periodicidad	Producto
	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
Implementación	Ejercer control sobre la operación	Realizar seguimiento y 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, gestión y recomendaciones del plan de privacidad y seguridad de la información	Implementar acciones	Anual	Informe de ejecución del plan de privacidad y seguridad de la información
	Gestionar incidentes de seguridad de la información	Gestionar los incidentes de seguridad de la información, garantizando su identificación, registro, análisis, atención y cierre oportuno, conforme a los lineamientos institucionales y con el fin de minimizar impactos sobre la información. Asimismo, la gestión de incidentes incluirá la documentación de lecciones aprendidas con el fin de prevenir su recurrencia.	Implementar mecanismos de reporte de incidentes, uso de herramientas o bitácoras de registro y/o análisis de causas.	Permanente / Cuando se presenten	Registro de incidentes de seguridad de la información, reportes de incidentes y acciones de tratamiento



Componente	Actividad	Descripción	Estrategia o mecanismo	Periodicidad	Producto
Evaluación	Elaborar plan de seguimiento y revisión del MPSI	Elaborar plan de seguimiento y revisión del MPSI	Reuniones de trabajo con el profesional de control y evaluación	Anual	Plan de seguimiento y revisión del MPSI
	Ejecutar el plan de seguimiento y evaluación del MPSI	Adelantar el seguimiento y evaluación del MPSI mediante el análisis del cumplimiento del plan de privacidad y seguridad de la información, la ejecución de auditorías internas y la verificación de los lineamientos establecidos.	Ejecutar plan de seguimiento y evaluación	Anual	Informe de seguimiento y evaluación del MPSI
Mejora continua	Socializar los resultados y definir acciones de mejora continua	Socializar los resultados de seguimiento 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 Institucional de Gestión y Desempeño y planes de mejoramiento definidos
	Realizar seguimiento a las acciones de mejora	Realizar seguimiento al cumplimiento de las acciones de mejora definidas, verificando su implementación y efectividad.	Revisión periódica de los planes de mejoramiento, verificación de evidencias, reportes de avance y mesas de trabajo con responsables de los procesos.	Anual o cuando se requiera	Informes de seguimiento a planes de mejoramiento

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.
2026-06-04	2	TS- 1215	<p>Actualización del formato del documento y ajuste de estructura. Además, se realizan ajustes en la redacción, organización de contenidos y actualización de los referentes normativos.</p> <p>Se actualizan los apartados de objetivo, alcance, definiciones, roles y responsabilidades y la fase de evaluación.</p> <p>Se incluye el numeral de gestión de activos de información y se actualizan las actividades para la implementación del Modelo de Privacidad y Seguridad de la Información (MPSI).</p>

Elaboración, revisión y aprobación	
Elaboración	
Nombre:	Camila Andrea Sánchez Amaya
Cargo:	Profesional especializado
Revisión	
Nombre:	Juan Stiven Ríos Andrade
Cargo:	Asesor
Aprobación	
Nombre:	Paola Patricia Rodríguez
Cargo:	Subdirectora Jurídica y de Gestión Institucional