Fondo Adaptación

Propuesta Plan de seguridad y privacidad de la información (MSPI)

2023-2026

Versión 5.0, enero 2026

Equipo Directivo Fondo Adaptación:

Angie Lizeth Rodríguez Fajardo
Gerente (E)

Lina Natalia Ramirez Rodriguez
Subgerente de Gestión del Riesgo

Jhonattan Julián Duque Murcia
Subgerente de Proyectos

Diana Marcela Ramírez Ayala
Subgerente de Estructuración (E)

Jorge Andrés Charry Gómez
Subgerente de Regiones

Alejandro Mario De Jesús Melo Saade
Secretario General

Diana Marcela Medina Henao
Jefe Oficina Asesora de Planeación y Cumplimiento

Investigación y textos:

EQUIPO DE TRABAJO
Tecnologías de la información

Plan de seguridad y privacidad de la información (MSPI) 2023-2026

Versión 5.0 Enero 2026, Bogotá D.C.

CONTROL DE CAMBIOS Y NOMENCLATURA

VERSIÓN	FECHA	DESCRIPCIÓN
1.0	2022/09	Documento Inicial
1.1	2023/02	Documento Ajustado alcance, objetivos
2.0	2023/05	Modificación estructura orgánica, inclusión calendario seguridad y actualización servicios tecnológicos
3.0	2024/01	Actualización según lineamientos planeación 2024, revisión de cronograma 2024, aprobado en el Comité Institucional de Gestión y Desempeño (CIGD) del 26 y 29 de enero de 2024.
4.0	29/01/2025	Actualización del Plan de seguridad y privacidad de la información (MSPI) 2023-2026, aprobado en el Comité Institucional de Gestión y Desempeño (CIGD) del 28 y 29 de enero de 2025.
5.0	XX/01/2026	Actualización del Plan de seguridad y privacidad de la información (MSPI) 2023-2026, aprobado en el Comité Institucional de Gestión y Desempeño (CIGD) del XX de enero de 2026.

Tabla de contenido

1 INTRODUCCIÓN

El Modelo de Seguridad y Privacidad de la Información (MSPI) se compone de las fases de diagnóstico, planeación, implementación, verificación y actuar, y a través de la implementación del Sistema de Gestión de Seguridad de la Información (en adelante SGSI) se cumple con lo requerido y exigido en los lineamientos y directrices emitidas por MinTIC.

Dentro del Sistema de Gestión de Seguridad de la Información, se contemplan grandes conjuntos de actividades dentro de cada una de las fases como son:

- Diagnóstico y Planificación: Se realiza una validación inicial del estado del MSPI, con el fin de identificar la brecha y las acciones que se deben ejecutar para su mitigación, donde se desarrollan los planes de implementación que involucran actividades como: Actualización o elaboración de la documentación, sensibilización y capacitación, identificación y clasificación de los activos de información, identificación, valoración y gestión y tratamiento del riesgo de seguridad digital, entre otras a desarrollar en estas fases.
- Implementación: Se realiza la implementación de los planes definidos en lase anterior como son tratamiento de riesgos, sensibilización, capacitación e implementación de controles.
- Verificación: Revisiones del sistema, auditorías internas y externas.
- Actuar: Monitoreo, revisión y mejora para las actividades propias de SGSI.

Este plan está enfocado a las actividades que realizara el FONDO para la implementación de dicho Modelo.

2 DEFINICIONES

- **MSPI:** Modelo de seguridad y privacidad de la información.
- **MGRSI:** Modelo Nacional de Gestión de Riesgos de Seguridad Digital.
- **MGRSD:** Modelo nacional de gestión de riesgos de seguridad digital.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **Confidencialidad:** propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- **Disponibilidad:** propiedad de la información de ser accesible, utilizable y recuperable a demanda por una entidad.
- **Estándar:** Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. En este documento se habla de las Norma Técnica Colombiana ISO27001:2022 e ISO31000:2019.
- **Gestión de riesgos:** Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información

de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

- **Incidente de seguridad de la información:** Resultado de intentos intencionales o accidentales de romper las medidas de seguridad de la información impactando en la confidencialidad, integridad o disponibilidad de la información.
- **Integridad:** propiedad de la información de ser completa, exacta e inalterada exactitud y completitud.
- **Información:** Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y trasmitirla.

3 FONDO ADAPTACIÓN (campo obligatorio – diligencia OAPC)

Incluye que es el Fondo, Adaptación, misión, visión, mapa de procesos, entre otros. Texto estándar para todos los planes. Lo diligencia únicamente la Oficina Asesora de Planeación y Cumplimiento.

Objetivos estratégicos

El Fondo Adaptación contempla dos perspectivas en su planeación acordes con el perfil de los resultados a lograr en los objetivos estratégicos establecidos Plan Estratégico Institucional: la **perspectiva externa**, en la cual se contempla el punto de vista del beneficiario de los proyectos e iniciativas ejecutadas por el Fondo (Misional y Transversal) y la **perspectiva interna**, desde el que se contempla los resultados del cliente interno (Transversal). Los objetivos estratégicos (OE) 2023 -2026 por cada perspectiva son los siguientes:

PERSPECTIVA EXTERNA
OE1. Identificar, estructurar y ejecutar proyectos de restauración ecológica y ordenamiento territorial para el aprovechamiento de la diversificación productiva fomentando la economía circular, la conservación de las fuentes hídricas y el manejo adecuado de residuos sólidos que contribuyan a la adaptación al cambio climático en los territorios.
OE2. Identificar, estructurar y gestionar proyectos que contribuyan a la reducción del riesgo, la adaptación al cambio climático y la recuperación post-desastre.
OE3. Adoptar e implementar estrategias para la recuperación y fortalecimiento socioeconómico del territorio, de manera que estas, le permitan a la población una adaptación sostenible al cambio climático.

PERSPECTIVA EXTERNA
OE4. Identificar y promover iniciativas locales para la adaptación al cambio climático y la prevención y gestión del riesgo, propiciando la transformación de hábitos y costumbres en la forma de habitar los territorios para: el acceso al agua, al suelo y a la vivienda; a la accesibilidad, la movilidad y la conectividad; y a espacios para la salud, la educación y la cultura; fortaleciendo procesos sociales desde el encuentro y la participación comunitaria, en el marco del derecho a un hábitat digno, fortalecimiento la atención del fenómeno de la niña (2010-2011) en el área de infraestructura, fomentando su integración en el territorio con las nuevas estrategias para la adaptación al cambio climático y la prevención y gestión del riesgo.
PERSPECTIVA INTERNA
OE5. Fortalecer una cultura organizacional orientada al relacionamiento eficaz con los usuarios, al desarrollo del talento humano y a la modernización de la gestión del Fondo Adaptación.

En tal sentido, la perspectiva de planeación es el punto de vista desde el cual se programa y hace seguimiento y análisis para el cumplimiento de los objetivos estratégicos de la Entidad.

4 ANÁLISIS DE CONTEXTO

El Fondo Adaptación se encuentra en un nivel inicial de madurez en la implementación del SGSI, evidenciado en los resultados del FURAG 2024, donde el componente de Seguridad Digital alcanzó un **70%.** Este resultado refleja avances importantes, pero también la necesidad de fortalecer controles, procesos y capacidades institucionales en seguridad de la información.

El contexto normativo es altamente exigente, dado el marco legal vigente en materia de protección de datos personales, seguridad digital y gobierno digital, lo cual obliga a la entidad a implementar modelos formales como el MSPI y el MGRSD. Adicionalmente, la entidad gestiona información crítica asociada a proyectos de infraestructura, gestión del riesgo y atención post-desastre, lo que incrementa la exposición a riesgos de seguridad de la información.

En este escenario, el Plan de Seguridad y Privacidad de la Información se convierte en un instrumento estratégico para elevar el nivel de madurez del SGSI, fortalecer la cultura organizacional en seguridad digital y asegurar el cumplimiento institucional hacia el año 2026 se espera alcanzar un **90%** de nivel de implementación, siempre y cuando se cuente con todos los recursos necesarios para la implementación y operación del Sistema de Gestión de Seguridad de la Información.

5 OBJETIVO

Implementar y fortalecer el Modelo de Seguridad y Privacidad de la Información (MSPI) y el Sistema de Gestión de Seguridad de la Información (SGSI) en el Fondo Adaptación, garantizando la confidencialidad, integridad y disponibilidad de la información, mediante la gestión adecuada de los riesgos de seguridad digital y el cumplimiento de los lineamientos definidos por el Ministerio TIC, durante el periodo 2023-2026

6 ALCANCE

El Plan de Seguridad y Privacidad de la Información de la entidad toma como referencia el Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MGRSI) y el Modelo de Seguridad y Privacidad de la Información (MSPI), ambos del Ministerio de las TIC como órgano regulador en la materia. Existe una interacción entre estos dos modelos que se puede ver en la Figura 1.

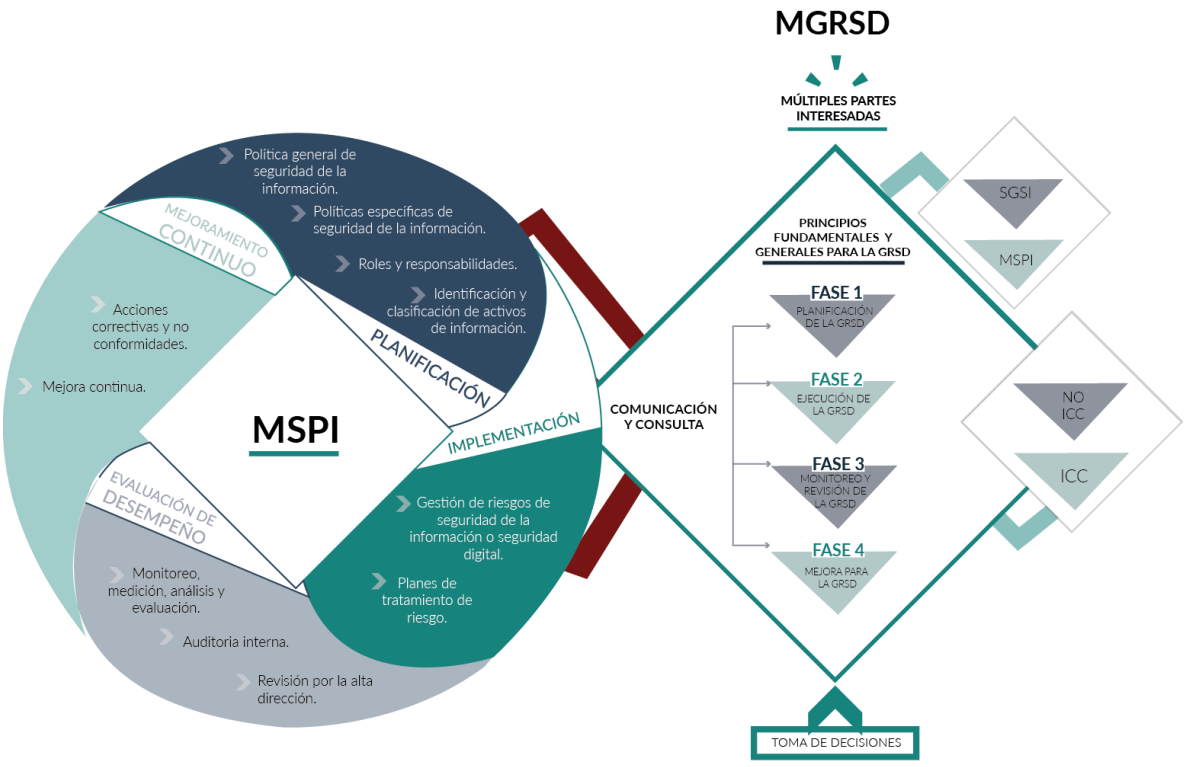

Figura 1 Interacción entre el MSPI y el MGRSD.
Fuente: MinTIC.

El alcance en el Plan de Seguridad y Privacidad de la Información abarca la planificación, el diagnóstico, planeación, implementación, verificación y actuar

del MSPI y SGSI, así como la planificación, la ejecución, el monitoreo, revisión y mejora de todas las fases del MGRSI.

El alcance del plan aplica para todo el personal de planta, contratista y terceros cuando es el caso, el cual se evidencia en el siguiente link:

https://drive.google.com/drive/folders/1P_7__1HM4IY5FBgjQJd85nZReXKeIj4u

7 MARCO NORMATIVO

Define a quién va dirigido o aplica el plan. Son las limitaciones o campo de aplicación del documento, describe la cobertura de las disposiciones en términos de procesos, cargos, áreas. Se recomienda utilizar expresiones como: Esta política se aplica en las áreas de …

7.1 Marco Legal

A continuación, se enumera la normativa legal (Leyes, Decretos y similares) que se cumple con este plan:

- Ley 23 de 1982 de Propiedad Intelectual - Derechos de Autor
- Ley 1032 de 2006, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1266 de 2007, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.
- Ley 1437 de 2011, "Código de procedimiento administrativo y de lo contencioso administrativo".
- Ley 1581 de 2012, "Protección de Datos personales".
- Decreto 2609 de 2012, por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011.
- Decreto 1377 de 2013, por la cual se reglamenta la ley 1581 de 2012.
- Ley 1712 de 2014, "De transparencia y del derecho de acceso a la información pública nacional".
- Decreto 1078 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Ley 962 de 2005. "Simplificación y Racionalización de Trámite. Atributos de seguridad en la Información electrónica de entidades públicas;"
- Ley 1150 de 2007. "Seguridad de la información electrónica en contratación en línea".
- Ley 1341 de 2009. "Tecnologías de la Información y aplicación de seguridad".

- Decreto 2952 de 2010. "Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008".
- Decreto 886 de 2014. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012".
- Decreto 1008 de 2018 "por la cual se establecen los lineamientos generales para la Política de Gobierno Digital…"
- Decreto 1083 de 2015. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012".
- CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016 Política Nacional de Seguridad Digital.
- Resolución Número 00500 DE MARZO 10 DE 2021
- Resolución 746 de 2022 Modelo de Seguridad y Privacidad de la Información.
- Directiva Presidencial 02 "Para garantizar la implementación segura de la Política de Gobierno Digital liderada por el Ministerio de Tecnologías de la Información y las comunicaciones (MinTIC)"

7.2 Requisitos Técnicos

A continuación, se relacionan las normas técnicas tenidas en cuenta:

- Modelo de Seguridad y Privacidad de la Información – MINTIC.
- Modelo Nacional de Gestión de Riesgos de Seguridad Digital – MINTIC.
- Norma Técnica Colombiana NTC/ISO 27001:2022 Sistemas de gestión de la seguridad de la información.
- Norma Técnica Colombiana NTC/ISO 17799 Código de práctica para la gestión de la seguridad.

8 FORMULACIÓN DEL PLAN O PROGRAMA

La formulación de los planes y metas estratégicas debe incluir como mínimo los siguientes ítems, de acuerdo con lo establecido en el Anexo No. 2 Lineamientos para la Formulación de Planes Institucionales Vigencia 2026.

8.1 Objetivo estratégico

Fortalecer la gestión institucional de la seguridad y privacidad de la información mediante la implementación progresiva del Modelo de Seguridad y Privacidad de la Información (MSPI) y el Sistema de Gestión de Seguridad de la Información (SGSI), contribuyendo al cumplimiento de los objetivos estratégicos internos del Fondo Adaptación y a la modernización de su gestión institucional

8.2 Estrategias

- Implementar de manera gradual las fases del MSPI: diagnóstico, planeación, implementación, verificación y mejora continua.
- Identificar, analizar y tratar los riesgos de seguridad digital a través del Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MGRSD).
- Actualizar y fortalecer la documentación del SGSI (políticas, procedimientos, guías y formatos).
- Ejecutar planes de sensibilización y capacitación en seguridad de la información para funcionarios, contratistas y terceros.
- Implementar y mantener controles técnicos, administrativos y operativos que mitiguen los riesgos identificados.
- Realizar auditorías internas y externas para evaluar el desempeño y madurez del SGSI

8.3 Metas

- Alcanzar un 90% de nivel de implementación del SGSI en el año 2026.
- Ejecutar anualmente el autodiagnóstico del MSPI y cerrar las brechas identificadas.
- Actualizar de forma anual las políticas de seguridad de la información y protección de datos personales.
- Gestionar el 100% de los riesgos de seguridad de la información identificados.
- Implementar planes de sensibilización y capacitación en seguridad de la información cada vigencia.
- Realizar auditorías anuales al SGSI y ejecutar los planes de mejoramiento resultantes

8.4 Responsables

- **Alta Dirección:** Definición de lineamientos y respaldo institucional.
- **Equipo de Tecnologías de la Información:** Articulación técnica y operativa del MSPI y SGSI.
- **Profesional de Seguridad de la Información:** Implementación, seguimiento y mejora del SGSI.
- **Oficina Asesora de Planeación y Cumplimiento:** Revisión, aprobación y seguimiento.
- **Líderes de Proceso:** Gestión de riesgos y aplicación de controles en sus áreas.

8.5 Indicadores

- Porcentaje de avance en la implementación del MSPI.
- Nivel de madurez del SGSI según resultados FURAG.
- Porcentaje de riesgos de seguridad de la información gestionados.
- Número de incidentes de seguridad de la información registrados y gestionados.
- Porcentaje de cumplimiento del cronograma de actividades del MSPI.

- Número de funcionarios y contratistas capacitados en seguridad de la información.
- Resultados de auditorías internas y externas del SGSI

8.6 Lineamientos para la implementación del plan

La alta dirección a través del Equipo de trabajo de tecnologías de la información y teniendo en cuenta la política de seguridad digital de la entidad dará las directrices para la implementación del Modelo de Seguridad y Privacidad de la Información, Modelo de Gestión de Riesgos de Seguridad y Privacidad de la Información y el Sistema de Gestión de Seguridad de la Información.

El Equipo de trabajo de tecnologías de la información debe articular, con la dirección de entidad, los esfuerzos, recursos, metodologías y estrategias para asegurar la implementación de los Modelos y Sistemas.

La Alta Dirección designará un representante ante el Sistema de Gestión de Seguridad de la Información y al responsable de la seguridad de la información de la entidad; mientras no exista una designación explicita diferente el líder del Equipo de Trabajo de Tecnologías de la Información tendrá a su cargo ambos responsabilidades, quien a su vez se apoyará en expertos técnicos para la implementación, puesta en marcha, mantenimiento, supervisión y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

8.7 Modelo De Seguridad Y Privacidad De La Información - MSPI

El Modelo de Seguridad y Privacidad de la Información (MSPI) desarrollado por MINTIC, contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de los activos información. En la figura 2 se presenta el ciclo de operación.

El MSPI propone unas metas, indicadores, documentación e instrumentos que deben ser ejecutados de acuerdo con unos lineamientos y guías que propone el Ministerio de las TIC, basado en las mejores prácticas en la materia.

Este modelo conduce a la preservación de la confidencialidad, integridad y disponibilidad de la información y los datos, mediante la aplicación de un adecuado proceso de gestión del riesgo y operación del Sistema de Gestión de Seguridad de la Información brindado confianza y seguridad a las partes interesadas.

Figura 2 Ciclo de operación del Modelo de Seguridad y Privacidad de la Información
Fuente: MINTIC

8.8 Modelo Nacional De Gestión De Riesgos De Seguridad Digital – MGRSD

Este modelo fue desarrollado y propuesto por MINTIC, para dar cumplimiento a la política nacional de seguridad establecida en el documento CONPES 3854 del 11 de abril de 2015. El modelo está orientado a incrementar la conciencia ciudadana y las capacidades del Gobierno y de las empresas en general, con el fin de identificar, analizar, evaluar y tratar los riesgos de seguridad digital.

En este modelo también se presentan guías para la gestión del riesgo de seguridad digital según el tipo de sector. (Gobierno nacional, territoriales y sector público; sector privado y mixto; sector fuerza pública y ciudadanía en general).

El MGRSD está estructurado como lo indica la Figura 3:

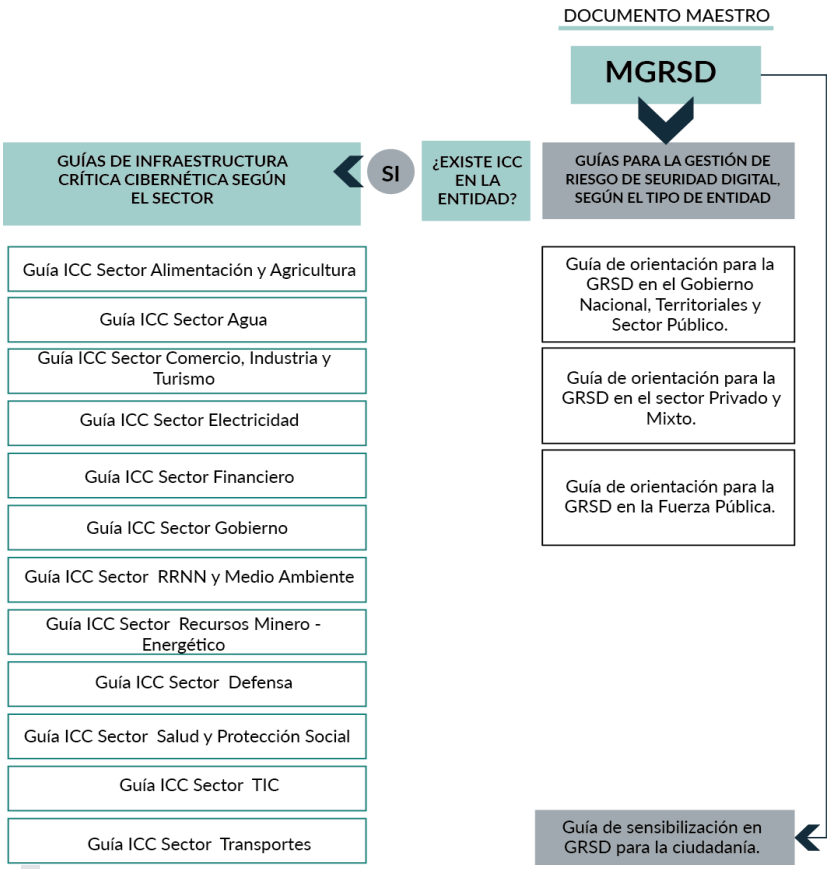

Figura 3 Modelo nacional de gestión de riesgos de seguridad digital
Fuente: MINTIC

El marco conceptual del modelo propone las fases que se presentan en la figura 4.

- **Planificación de la GRSD**: Consiste en la definición de contextos, variables para posterior análisis y evaluación de riesgos y en general todos los aspectos que se desarrollarán en los demás componentes.
- **Ejecución de la GRSD**: Consiste en el desarrollo de las actividades para el análisis y evaluación de los riesgos de seguridad digital, se identifican aspectos inherentes y residuales de los mismos, así como la definición del tratamiento de los riesgos en el marco de la seguridad de la información y particularmente en las ICC.
- **Monitoreo y Revisión de la GRSD**: Consiste en la permanente evaluación que permita asegurar que dicha gestión se está llevando a cabo bajo los aspectos y lineamientos definidos por cualquier entidad para sus riesgos de seguridad digital. Se desprenden aspectos de reporte y aseguramiento del seguimiento de todos los planes de tratamiento que se derivan de su aplicación.
- **Mejora de la GRSD:** Componente que tiene una orientación para establecer los mecanismos que permitan alcanzar un mayor grado de madurez de la GRSD en cualquier entidad. El mejoramiento continuo se estará dando de forma progresiva en la medida que se cumplan con los objetivos de la GRSD;

así como la definición y aplicación modelos de evaluación de riesgos de seguridad digital con una orientación menos subjetiva y basada en modelos matemáticos que brinden mayor exactitud en la medición de las variables de impacto de los riesgos de seguridad digital sobre los activos de información y las ICC identificadas.

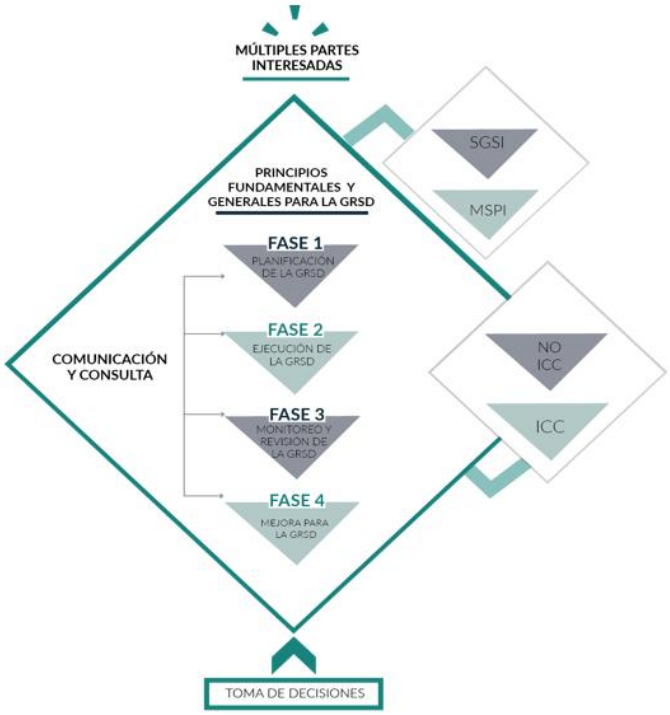

Figura 4 Fase modelo nacional de gestión de riesgos de seguridad digital
Fuente: MINTIC

8.9 Política y Lineamientos De Gestión Del Riesgo En El Fondo De Adaptación

La política y lineamientos de gestión del riesgo en el Fondo Adaptación integran un proceso de gestión del riesgo de manera transversal en toda la gestión de la entidad, en sus activos de información, políticas de operación y en general en la cultura organizacional. Incluye además los planteamientos legales y reglamentarios referidos a la gestión del riesgo de seguridad digital, de acuerdo con el Anexo 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas. En el siguiente vínculo se puede consultar la política:

https://drive.google.com/file/d/15RjZBzZPUgHOwGUlr2DqCIfa7ZlbX746/view?usp=sharing

8.10 Actividades del Plan De Seguridad y Privacidad de la Información y del Plan de Tratamiento de Riesgos

De acuerdo con los modelos anteriormente descritos y la política y lineamientos de gestión del riesgo del Fondo Adaptación, se proponen el cronograma de actividades anexo para la implementación del Modelo de Seguridad y Privacidad de la Información y el Sistema de Gestión de Seguridad de la Información.

El cronograma de actividades se presenta como un anexo a este documento.

8.11 Presupuesto

La presente contratación se suscribirá con cargo a los gastos operativos por concepto de "Contratos de Estudio y Apoyos Transversales" del Proyecto de Inversión 2019011000191 "Reconstrucción de zonas e infraestructuras afectadas por la ocurrencia del fenómeno de la Niña 2010-2011. Nacional", cuyo objetivo es "Reconstruir zonas e infraestructuras afectadas por la ocurrencia del fenómeno de La Niña 2010-2011, el cual fue declarado de importancia estratégica por el documento CONPES 3776 de 2013".

De acuerdo con lo establecido en el parágrafo segundo del artículo 5º del Decreto Ley 4819 de 2010, con cargo a los recursos señalados en el citado decreto se pueden financiar gastos operativos y administrativos, entre los cuales, de acuerdo con lo aprobado por el Consejo Directivo de la Entidad se encuentra la línea de los Contratos de Estudio y Apoyos Transversales. De acuerdo con la cadena de valor del proyecto, estos gastos se incluyen transversalmente en el costo de los productos.

9 REFERENCIAS

- 1-PET-P-01 Política y Lineamientos para la gestión de calidad
- 1-PET-P-02 Política y Lineamientos para la gestión del riesgo
- 1-PET-P-03 Política y Lineamientos para la gestión de resultados
- 5-PAT-P-01 Política de gobierno digital
- 5-PAT-P-02 Política de gestión y gobierno de datos

10 ANEXOS

10.1 Anexo 1 Cronograma mensual de actividades

CRONOGRAMA PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION				
Ítem	**Gestión / Proyecto**	**Actividades**	**Responsables**	**Fechas Programación Tareas 2026** **Desarrollo de la actividad**
1	Autodiagnóstico del MSPI	Realizar actualización de autodiagnóstico anual, con el	Profesional de Seguridad de	Primer

CRONOGRAMA PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION				
Ítem	**Gestión / Proyecto**	**Actividades**	**Responsables**	**Fechas Programación Tareas 2026** **Desarrollo de la actividad**
		fin de identificar brechas y las acciones para su mitigación.	la Información	Semestre
		Definir controles de mitigación y cierre de brechas en cada vigencia para avanzar en la implementación del MSPI	Profesional de Seguridad de la Información	Primer Semestre
		Implementación de controles definidos para la mitigar las brechas de seguridad.	Profesional de Seguridad de la Información Procesos de la Entidad	Durante la vigencia 2026
		Revisar el cumplimiento de los controles de acuerdo con la política de seguridad.	Profesional de Seguridad de la Información	Durante la vigencia 2026
2	Políticas de Seguridad de la Información	Formalización de la actualización de la política de seguridad de la información	Profesional de Seguridad de la Información	Primer Semestre
		Revisión de la política de seguridad de la información	Oficina de Planeación y Cumplimiento.	Primer Semestre
		Aprobación por el comité Institucional de Gestión y Desempeño.	Comité Institucional de Gestión y Desempeño	Primer Semestre
3	Gestión de Activos de Información	Revisar la documentación anual frente a la normativa vigente y actualizarla de ser necesario.	Profesional de Seguridad de la Información	Durante la vigencia 2026
		Realiza identificación y actualización anual de los Activos de Información.	Profesional de Seguridad de la Información	Durante la vigencia 2026
		Realizar clasificación anual de los activos de información.	Profesional de Seguridad de la Información	
		Socialización de activos de información anual	Profesional de Seguridad de la Información	Segundo Semestre
4	Gestión de Riesgos	Realizar gestión de riesgos de seguridad de la información.	Profesional de Seguridad de la Información	Segundo Semestre

CRONOGRAMA PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION				
Ítem	**Gestión / Proyecto**	**Actividades**	**Responsables**	**Fechas Programación Tareas 2026** **Desarrollo de la actividad**
		Definir plan de tratamiento de riesgos con los procesos de los activos críticos de la Entidad.	Profesional de Seguridad de la Información. Líderes de Proceso Líder del E.T. Tecnologías	Segundo Semestre
		Monitorización de los riesgos	Oficina de Planeación y Cumplimiento.	Durante la vigencia 2026
5	Gestión de Incidentes de Seguridad de la Información	Revisar y actualizar anualmente la documentación de Gestión de Incidentes (guía, procedimiento y formatos)	Profesional de Seguridad de la Información	Durante la vigencia 2026
		Gestionar los incidentes de Seguridad de la Información identificados permanenteme nte.	Profesional de Seguridad de la Información	
		Documentar los incidentes de seguridad presentados.	Profesional de Seguridad de la Información	
6	Plan de sensibilización y capacitación en seguridad de la información	Elaborar y ejecutar el plan de sensibilización y capacitación anual en seguridad de la información	Profesional de Seguridad de la Información	Durante la vigencia 2026
7	Requisitos Legales de Seguridad de la Información	Identificar la normativa vigente en materia de seguridad que aplica a la organización en cuanto a requisitos legales cuando sea requerido	Profesional de Seguridad de la Información	Durante la vigencia 2026 O cuando sea requerido
		Realizar actualización del normograma de la Entidad en cada vigencia.		
		Gestionar la publicación del normograma	Oficina Asesora de Planeación	Durante la vigencia 2026 O cuando sea requerido
8	Continuidad de las Operaciones	Definir o actualizar anualmente el plan de continuidad de las	Profesional de Seguridad de la Información	Durante la vigencia 2026

CRONOGRAMA PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION				
Ítem	**Gestión / Proyecto**	**Actividades**	**Responsables**	**Fechas Programación Tareas 2026**
				Desarrollo de la actividad
		operaciones.		
		Diseñar y gestionar las pruebas al plan de continuidad de las operaciones.	Profesional de Seguridad de la Información Profesionales de Infraestructura	Durante la vigencia 2026
		Documentar las pruebas realizadas.	Profesional de Seguridad de la Información	
9	Protección de Datos Personales	Revisar y actualizar anualmente la política de Protección de Datos Personales.	Responsable de Protección de Datos Personales.	Durante la vigencia 2026
			Profesional de Seguridad de la Información	
10	Implementación de controles	Renovación de herramientas de seguridad adquiridas	Profesional de Seguridad de la Información	Durante la vigencia 2026
		Gestionar la adquisición anual de pruebas de ingeniería social	Responsable del E.T. Tecnologías	Durante la vigencia 2026
		Ejecutar prueba de ingeniería social	Responsable del E.T. Tecnologías	Durante la vigencia 2026
		Documentar el informe de las pruebas	Responsable del E.T. Tecnologías	Durante la vigencia 2026
		Socializar los resultados	Profesional de Seguridad de la Información	Durante la vigencia 2026
		Gestionar las campañas de sensibilización	Profesional de Seguridad de la Información	Durante la vigencia 2026
		Ejecutar campañas de sensibilización	Profesional de Seguridad de la Información	Durante la vigencia 2026
		Documentar el informe	Profesional de Seguridad de la Información	Durante la vigencia 2026
		Socializar los resultados	Profesional de Seguridad de la Información	Durante la vigencia 2026

CRONOGRAMA PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION				
Ítem	**Gestión / Proyecto**	**Actividades**	**Responsables**	**Fechas Programación Tareas 2026** **Desarrollo de la actividad**
		Adquisición y configuración de herramienta de gestión del SGSI	Profesional de Seguridad de la Información Líder del E.T. de Tecnologías	Durante la vigencia 2026
		Mantenimiento de la herramienta del SGSI	Profesional de Seguridad de la Información	Durante la vigencia 2026
		Ejecutar Pruebas de Seguridad tipo Análisis de Vulnerabilidades.	Profesional de Seguridad de la Información	Durante la vigencia 2026
		Diseñar e implementar los controles de seguridad.	Profesional de Seguridad de la Información.	Primer Semestre
11	Auditorías	Gestionar la adquisición de auditoría anual a seguridad de la información	Profesional de Seguridad de la Información	Durante la vigencia 2026
		Elaborar plan de mejoramiento	Profesional de Seguridad de la Información	Segundo Semestre
12	Indicadores SGSI	Definición, revisión y evaluación de los indicadores de medición del SGSI semestralmente.	Profesional de Seguridad de la Información	Durante la vigencia 2026
		Evaluación de los indicadores de Seguridad de la Información	Profesional de Seguridad de la Información	Durante la vigencia 2026