Fondo Adaptación

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

2025

Versión 4.0, enero 2025

Equipo Directivo Fondo Adaptación:

Carlos Alberto Carrillo Arenas
Gerente (E)

Julio Cesar Báez Cardozo
Subgerente de Gestión del Riesgo (E)

Julio Cesar Báez Cardozo
Subgerente de Proyectos (E)

Gerardo Andrés Trejos Ramírez
Subgerente de Estructuración (E)

Jorge Andrés Charry Gómez
Subgerente de Regiones

Diana Paola Páez Lozano
Secretaria General (E)

Gerardo Andrés Trejos Ramírez
Jefe Oficina Asesora de Planeación y Cumplimiento (E)

Investigación y textos:

EQUIPO DE TRABAJO
Tecnologías de la información

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

Versión 4.0 Enero 2025, 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	XX/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) de xxx xxxx (fecha)

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 OBJETIVO

3.1 Objetivo General

Generar el Plan de Tratamiento de Riesgos de la Entidad para definir la hoja de ruta en la mitigación de los riesgos y así fortalecer la confidencialidad, integridad y disponibilidad de la información en los activos críticos de la Entidad.

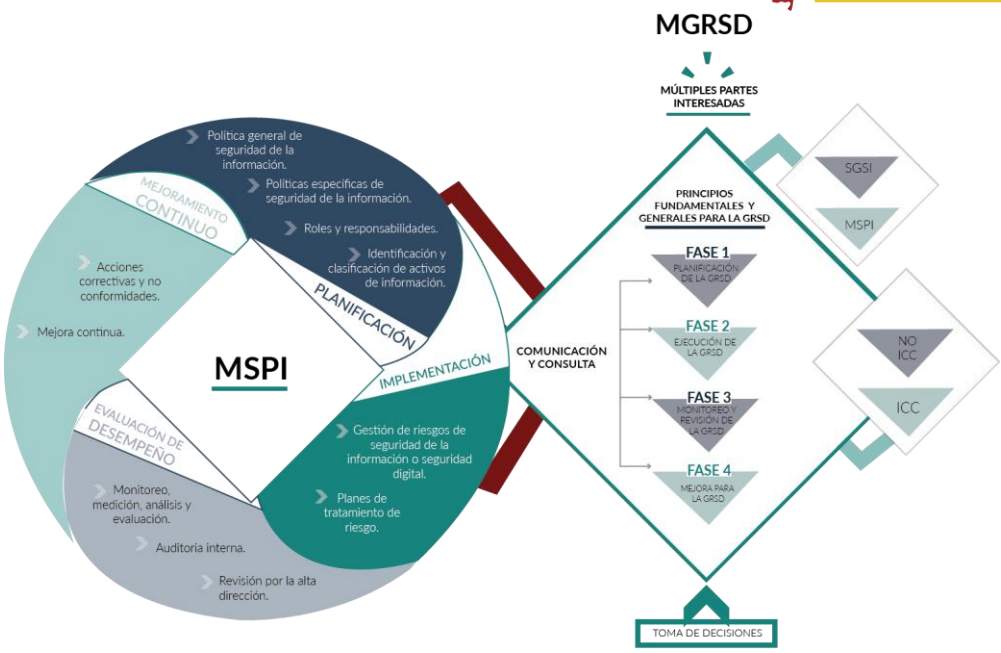
3.2 Objetivos específicos

- Realizar el contexto de los riesgos de seguridad de la información en articulación con la política establecida por la Entidad.
- Articular la gestión de riesgos y el plan de tratamiento con la Oficina de Planeación.
- Sensibilizar a los servidores públicos y contratistas de la Entidad acerca de la Gestión de Riesgos de Seguridad de la Información.

4 ALCANCE

El plan aplica para todo el personal de planta, contratista y terceros cuando es el caso. 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 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.



Es importante mencionar que la Entidad tiene una Política de Seguridad de la Información desde el año 2014 y que se ha actualizado periódicamente.

5 LINEAMIENTOS PARA IMPLEMENTACIÓN

La alta dirección a través del Equipo de trabajo de tecnologías de la información 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, con base en los lineamientos de la política de seguridad de la información de la entidad.

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

La Gerencia 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).

6 MARCO NORMATIVO

El siguiente es el Marco Normativo sobre el que se define el accionar estratégico de la entidad[1]:

6.1 Marco legal

- 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.

[1] Normograma

- 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)"

6.2 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.

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.

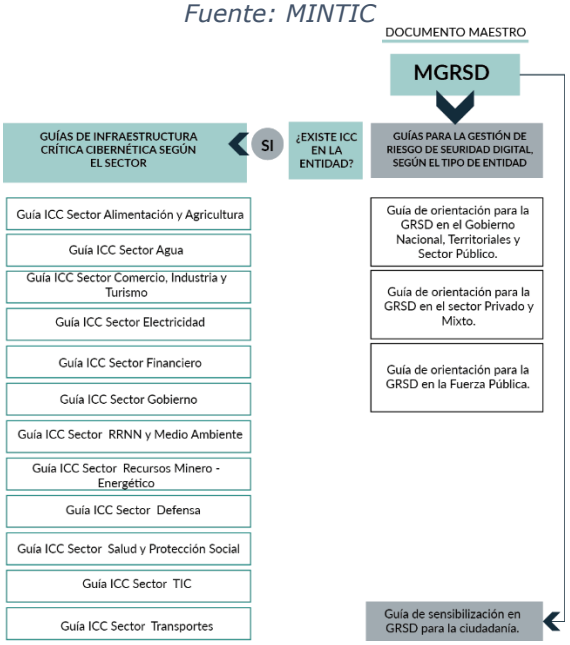
Figura 2 Ciclo de operación del Modelo de Seguridad y Privacidad de la Información
Fuente: MINTIC

8 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, en esta fase se realizan entrevistas con los responsables de cada área, con el fin de identificar los riesgos.

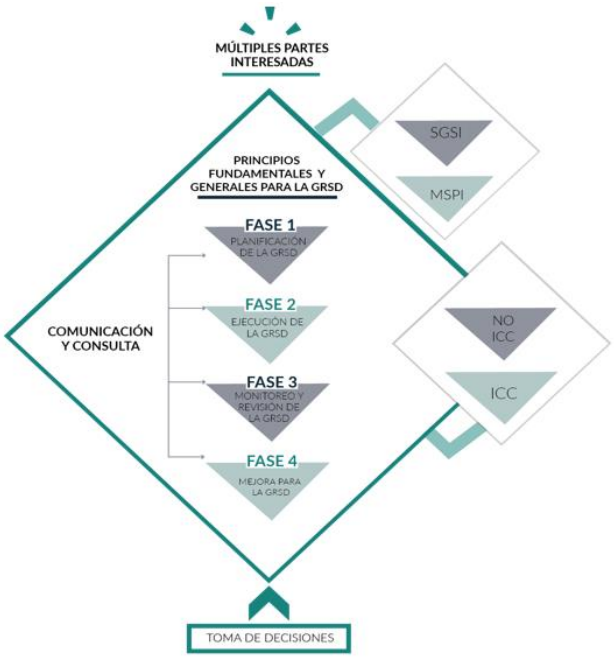
- **Ejecución de la GRSD**: Consiste en el desarrollo de las actividades para el análisis y evaluación de los riesgos de seguridad digital, se identifican aspectos inherentes y residuales de los mismos, así como la definición del tratamiento de

los riesgos en el marco de la seguridad de la información y particularmente en las ICC, en esta sección se realiza socialización con los responsables de los riesgos y se aceptan por parte de los líderes del proceso.

- **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, en esta sección se realiza el monitoreo por parte de los responsables de la revisión de riesgos de la Entidad.

- **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



9 POLÍTICA Y LINEAMIENTOS DE GESTIÓN DEL RIESGO EN EL FONDO ADAPTACIÓN

La política y lineamientos para la gestión del riesgo del 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.

10 ACTIVIDADES DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y TRATAMIENTO DE RIESGOS

De acuerdo con los modelos anteriormente descritos y la política y lineamientos para la 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 en el anexo 1 de este documento.

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.

11.1 Resultados FURAG

Los resultados de la medición del FURAG para el componente de Seguridad Digital fue del 45.5%, si bien es cierto, el resultado no representa la meta que debemos cumplir, debido a que el Sistema de Gestión de Seguridad de la Información se encuentra en implementación y en nivel de madurez inicial; con

la ejecución del plan de trabajo establecido, cada año vamos a fortalecer el SGSI de aquí al 2026 este habilitador, donde para el año 2024 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.

12 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
-

13 ANEXOS

- Cronograma actividades 2025 MSPI

Anexo 1. Cronograma actividades MSPI

CRONOGRAMA PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN							
Ítem	Gestión / Proyecto	Actividades	Responsables	Fechas Programación Tareas			
				2025		2026	
				Fecha Inicio	Fecha Final	Fecha Inicio	Fecha Final
1	Autodiagnóstico del MSPI	Realizar actualización de autodiagnóstico anual, con el fin de identificar brechas y las acciones para su mitigación.	Profesional de Seguridad de la Información	Febrero	Febrero	Febrero	Febrero
		Definir controles de mitigación y cierre de brechas en cada vigencia para avanzar en la implementación del MSPI	Profesional de Seguridad de la Información Procesos de la Entidad	Marzo	Marzo	Marzo	Marzo
		Implementación de controles definidos para la mitigar las brechas de seguridad.	Profesional de Seguridad de la Información Procesos de la Entidad	Abril	Abril	Abril	Abril
		Realizar revisiones de cumplimientos de la implementación de los controles de seguridad.	Profesional de Seguridad de la Información Procesos de la Entidad Control Interno	Noviembre	Noviembre	Noviembre	Noviembre
2	Políticas de Seguridad de la Información	Elaboración y actualización anual del Manual de Políticas de Seguridad de la Información.	Profesional de Seguridad de la Información	Marzo	Abril	Marzo	Abril
		Revisión por la Oficina de Planeación	Responsable de Oficina de Planeación.	Abril	Mayo	Abril	Mayo

CRONOGRAMA PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN							
Ítem	Gestión / Proyecto	Actividades	Responsables	Fechas Programación Tareas			
				2025		2026	
				Fecha Inicio	Fecha Final	Fecha Inicio	Fecha Final
		Aprobación por el comité Intitucional de Gestión y Desempeño.	Comité Institucional de Gestión y Desempeño	Junio	Junio	Junio	Junio
		Publicación del manual de Políticas de Seguridad de la Información.	Oficina de Planeación.	Julio	Julio	Julio	Julio
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	Abril	Abril	Abril	Abril
		Realiza identificación y actualización anual de los Activos de Información.	Profesional de Seguridad de la Información	Mayo	Julio	Mayo	Julio
		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	Agosto	Agosto	Agosto	Agosto
4	Gestión de Riesgos	Realizar gestión de riesgos de seguridad de la información.	Profesional de Seguridad de la Información	Junio	Julio	Junio	Julio
		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	Agosto	Septiembre	Agosto	Septiembre

CRONOGRAMA PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN							
Ítem	Gestión / Proyecto	Actividades	Responsables	Fechas Programación Tareas			
				2025		2026	
				Fecha Inicio	Fecha Final	Fecha Inicio	Fecha Final
		Revisión y aprobación.	Oficina de Planeación.	Octubre	Octubre	Octubre	Octubre
		Publicación de los riesgos de seguridad de la información.	Oficina de Planeación.				
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	Mayo	Diciembre	Mayo	Diciembre
		Gestionar los incidentes de Seguridad de la Información identificados permanentemente.	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	Profesional de Seguridad de la Información	Marzo	Diciembre	Marzo	Diciembre
		información anual					
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	Febrero	Marzo	Febrero	Marzo
		Realizar actualización del normograma de la Entidad en cada vigencia.					
		Publicar el Normograma	Jurídica	Abril	Abril	Abril	Abril

CRONOGRAMA PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN							
Ítem	Gestión / Proyecto	Actividades	Responsables	Fechas Programación Tareas			
				2025		2026	
				Fecha Inicio	Fecha Final	Fecha Inicio	Fecha Final
8	Continuidad de las Operaciones	Definir o actualizar anualmente el plan de continuidad de las operaciones.	Profesional de Seguridad de la Información	Mayo	Julio	Mayo	Julio
		Diseñar y gestionar las pruebas al plan de continuidad de las operaciones.	Profesional de Seguridad de la Información Profesionales de Infraestructura	Agosto	Noviembre	Agosto	Noviembre
		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.	Abril	Agosto	Abril	Agosto
			Profesional de Seguridad de la Información				
10	Implementación de controles	Renovación de herramientas de seguridad adquiridas	Profesional de Seguridad de la Información	Marzo	Diciembre	Marzo	Diciembre
		Gestionar la adquisición anual de pruebas de ingeniería social	Proveedor o tercero	Abril	Mayo	Abril	Mayo
		Ejecutar prueba de ingeniería social	Proveedor o tercero	Mayo	Junio	Mayo	Junio
		Documentar el informe de las pruebas	Proveedor o tercero	Junio	Junio	Junio	Junio

CRONOGRAMA PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN							
Ítem	Gestión / Proyecto	Actividades	Responsables	Fechas Programación Tareas			
				2025		2026	
				Fecha Inicio	Fecha Final	Fecha Inicio	Fecha Final
		Socializar los resultados	Profesional de Seguridad de la Información	Julio	Julio	Julio	Julio
		Gestionar la campañas de sensibilización	Profesional de Seguridad de la Información	Mayo	Junio	Mayo	Junio
		Ejecutar campañas de sensibilización	Proveedor o tercero	Julio	Agosto	Julio	Agosto
		Documentar el informe	Proveedor o tercero	Septiembre	Septiembre	Septiembre	Septiembre
		Socializar los resultados	Profesional de Seguridad de la Información	Octubre	Octubre	Octubre	Octubre
		Renovación de herramientas de seguridad adquiridas	Profesional de Seguridad de la Información	Marzo	Junio	Marzo	Junio
		Gestionar la adquisición anual de pruebas de ingeniería social	Proveedor o tercero	Abril	Mayo	Abril	Mayo
		Adquisición y configuración de herramienta de gestión del SGSI	Profesional de Seguridad de la Información Proveedor o tercero	Mayo	Junio	Mayo	Junio
		Mantenimiento de la herramienta del SGSI	Profesional de Seguridad de la Información	Frebrero	Diciembre	Frebrero	Diciembre

CRONOGRAMA PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN							
Ítem	**Gestión / Proyecto**	**Actividades**	**Responsables**	**Fechas Programación Tareas**			
				2025		**2026**	
				Fecha Inicio	**Fecha Final**	**Fecha Inicio**	**Fecha Final**
		Ejecutar Pruebas de Seguridad tipo Análisis de Vulnerabilidades.	Proveedor o tercero	Marzo	Junio	Marzo	Junio
		Diseñar e implementar los controles de seguridad.	Profesional de Seguridad de la Información.	Agosto	Diciembre	Agosto	Diciembre
11	Auditorías	Gestionar la adquisición de auditoría anual a seguridad de la información	Profesional de Seguridad de la Información	Agosto	Septiembre	Agosto	Septiembre
		Ejecución de Auditoría Interna anual al SGSI	Control Interno Proveedor o Tercero	Octubre	Noviembre	Octubre	Noviembre
		Elaborar plan de mejoramiento	Control Interno Profesional de Seguridad de la Información	Noviembre	Noviembre	Noviembre	Noviembre
12	Indicadores SGSI	Definición, revisión y evaluación de los indicadores de medición del SGSI semestralmente.	Profesional de Seguridad de la Información	Febrero	Marzo	Febrero	Marzo
		Evaluación de los indicadores de Seguridad de la Información	Profesional de Seguridad de la Información	Marzo Junio Septiembre Diciembre	Marzo Junio Septiembre Diciembre	Marzo Junio Septiembre Diciembre	Marzo Junio Septiembre Diciembre
13	Certificación ISO 27001:2022	Realizar revisiones de los procesos que se van a postular para la certificación.	Profesional de Seguridad de la Información	-	-	-	-
		Realizar diagnóstico de los procesos seleccionados	Profesional de Seguridad	-	-	-	-

CRONOGRAMA PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN							
Ítem	**Gestión / Proyecto**	**Actividades**	**Responsables**	**Fechas Programación Tareas**			
				2025		**2026**	
				Fecha Inicio	**Fecha Final**	**Fecha Inicio**	**Fecha Final**
			de la Información				
		Aplicar las acciones de mejora.	Profesional de Seguridad de la Información Procesos	Enero	Diciembre	-	-
		Elaborar y/o actualizar la documentación requerida para la certificación.	Profesional de Seguridad de la Información Proceso de la Entidad	Frebrero	Junio	Febrero	Junio
14	Solicitud de otorgamiento de certificación ISO 27001:2022	Gestionar la auditoría de otorgamiento del certificado de la Norma ISO 27001:2022	Control Interno Profesional de Seguridad de la Información	-	-	Marzo	Mayo
		Ejecutar la auditoría de otorgamiento	Organismo de Certificación	-	-	Junio	Julio
		Definir plan de mejoramiento	Profesional de Seguridad de la Información Líderes de Procesos	-	-	Agosto	Septiembre
		Implementar el Plan de Mejoramiento	Profesional de Seguridad de la Información Líderes de Procesos	-	-	Septiembre	Diciembre

Fuente: Tecnologías de la Información