COLOMBIA POTENCIA DE LA VIDA

Fondo Adaptación

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACION 2023-2026

Versión 1.0, enero 2024

Equipo Directivo Fondo Adaptación:

Helga María Rivas Ardila
Gerente (E)

Helga María Rivas Ardila
Subgerente de Gestión del Riesgo

Paola María Miranda Morales
Subgerente de Proyectos

Gerardo Andrés Trejos Ramírez
Subgerente de Estructuración (E)

Jorge Andrés Charry Gómez
Subgerente de Regiones

Diana Paola Páez Lozano
Secretaria General (E)

Mario Delfín Ortiz Jiménez
Jefe Oficina Asesora de Planeación y Cumplimiento (E)

Investigación y textos:

EQUIPO DE TRABAJO
Tecnologías de la Información

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 2023-2026.

Versión 1.0 enero de 2024, Bogotá D.C.

CONTROL DE CAMBIOS Y NOMENCLATURA

VERSIÓN	FECHA	DESCRIPCIÓN
1.0	2024/101	Documento Inicial, aprobado en el Comité Institucional de Gestión y Desempeño (CIGD) del 26 y 29 de enero de 2024.

Tabla de contenido

ILUSTRACIONES

1 INTRODUCCIÓN

Con la evolución de la seguridad de la información y ciberseguridad, se ve necesario realizar una correcta y adecuada gestión de riesgos, por lo que el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) desarrolla el Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MGRSI) y el Departamento Administrativo de la Función Pública (DAFP) desarrolla en colaboración con MINTIC el anexo 4 para la gestión de riesgos de seguridad digital, esto son adoptados por el FONDO ADAPTACIÓN para la implementación de dicho Modelo y mitigar oportunamente los riesgos que son identificados en los activos críticos de la Entidad.

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 ISO27001:2013 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 ALCANCE

El Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MGRSI) y la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – Anexo 4 Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas, es así como el Modelo de Seguridad y Privacidad de la Información se articula con estos como se puede observar en la figura a continuación:

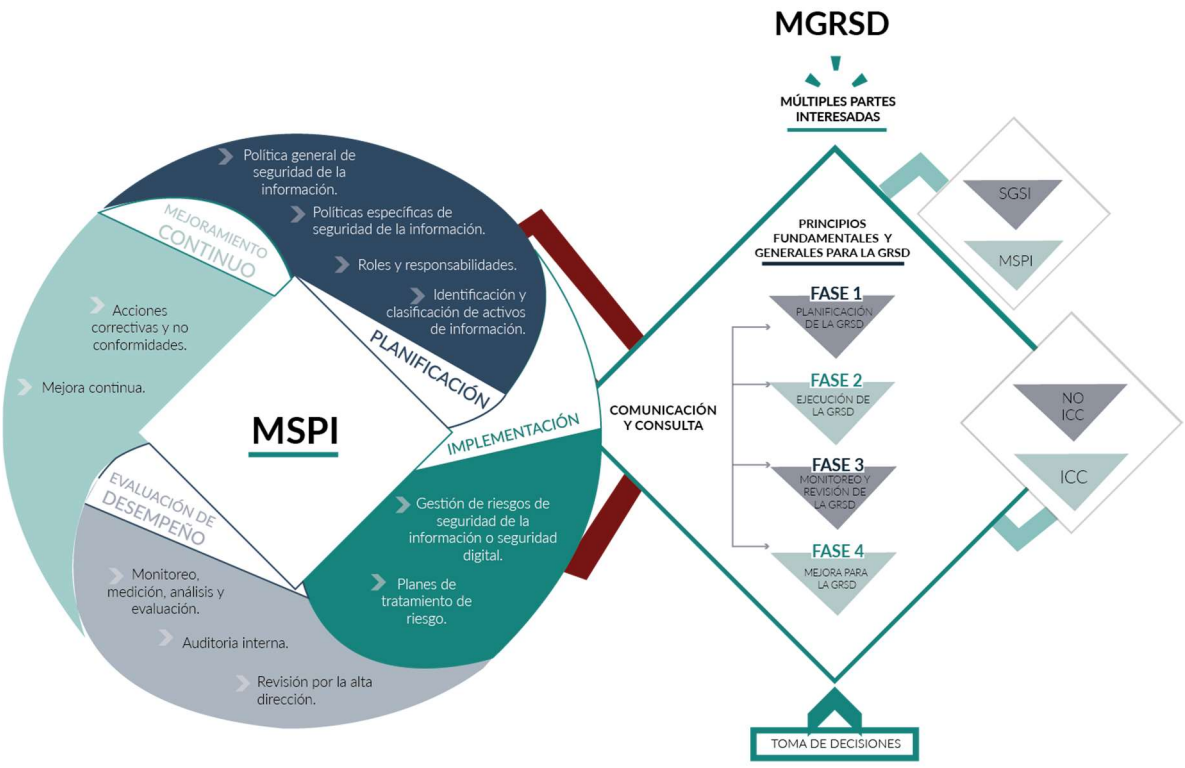

Ilustración 1 Interacción entre el MSPI y el MGRSD -Fuente MINTIC

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

4 ANÁLISIS DE CONTEXTO

En esta sección se realiza un entendimiento de la situación actual del plan de tratamiento de riesgos de seguridad en la Entidad:

4.1 Riesgos de Seguridad de la Información

En esta materia y de acuerdo con el levantamiento y gestión de riesgos de seguridad digital realizado en la vigencia 2023, se observan los siguientes avances:

- Se realiza identificación y clasificación de activos de información documental.
- Se identifican los activos documentales críticos.
- Se realiza gestión de riesgos, partiendo de los activos de información identificados.
- Se genera plan de tratamiento de riesgos para los que quedaron en una zona de riesgo alto.

4.2 Problemáticas

De acuerdo con el análisis del entendimiento estratégico y la madurez en seguridad de la entidad y la implementación del Modelo de Seguridad y Privacidad de la Información en cada uno de sus dominios, se pueden identificar las siguientes problemáticas:

ID	Descripción	Dominio
1	Falta terminar la identificación de activos de información tipo personas, hardware, software, servicios, seguridad y redes.	Seguridad y Privacidad
2	Falta finalizar el análisis de riesgos en los procesos, partiendo del total de activos críticos identificados en la Entidad.	Seguridad y Privacidad
3	Actualizar la matriz de riesgos de seguridad a la nueva normativa interna emitida por Planeación.	Seguridad y Privacidad
4	El área de TI se considera un área operativa más no estratégica.	Seguridad y Privacidad
5	Falta sensibilización y capacitación en riesgos de Seguridad Digital con todos los Líderes de Procesos.	Seguridad y Privacidad
6	Falta gestionar la implementación del plan de tratamiento de riesgos de seguridad de la información.	Seguridad y Privacidad

Ilustración 2 Problemáticas

4.3 Resultados FURAG

Los resultados 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 **70%** de nivel de implementación, teniendo en cuenta los recursos necesarios para la ejecución y operación del Sistema de Gestión de Seguridad de la Información y lo cual se encuentra descrito en el plan de mejoramiento establecido y donde se pueden observar las acciones que se llevaran a cabo para su cumplimiento.

5 OBJETIVOS

5.1 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.

5.2 Objetivos específicos

- Realizar gestión de riesgos de seguridad de la información para todos los activos críticos de la Entidad.
- Gestionar los riesgos de seguridad de la información para mantenerlos en niveles aceptables.

- Sensibilizar a los servidores públicos y contratistas de la Entidad acerca de la Gestión de Riesgos de Seguridad de la Información.

6 LINEAMIENTOS PARA 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 emite las directrices para el Modelo de Gestión de Riesgos de Seguridad y Privacidad de la Información.

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

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).

7 MARCO NORMATIVO

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

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 27001:2013 y 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.
- Guía para la Administración del Riesgo y el diseño de controles en entidades públicas de 2022.

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:

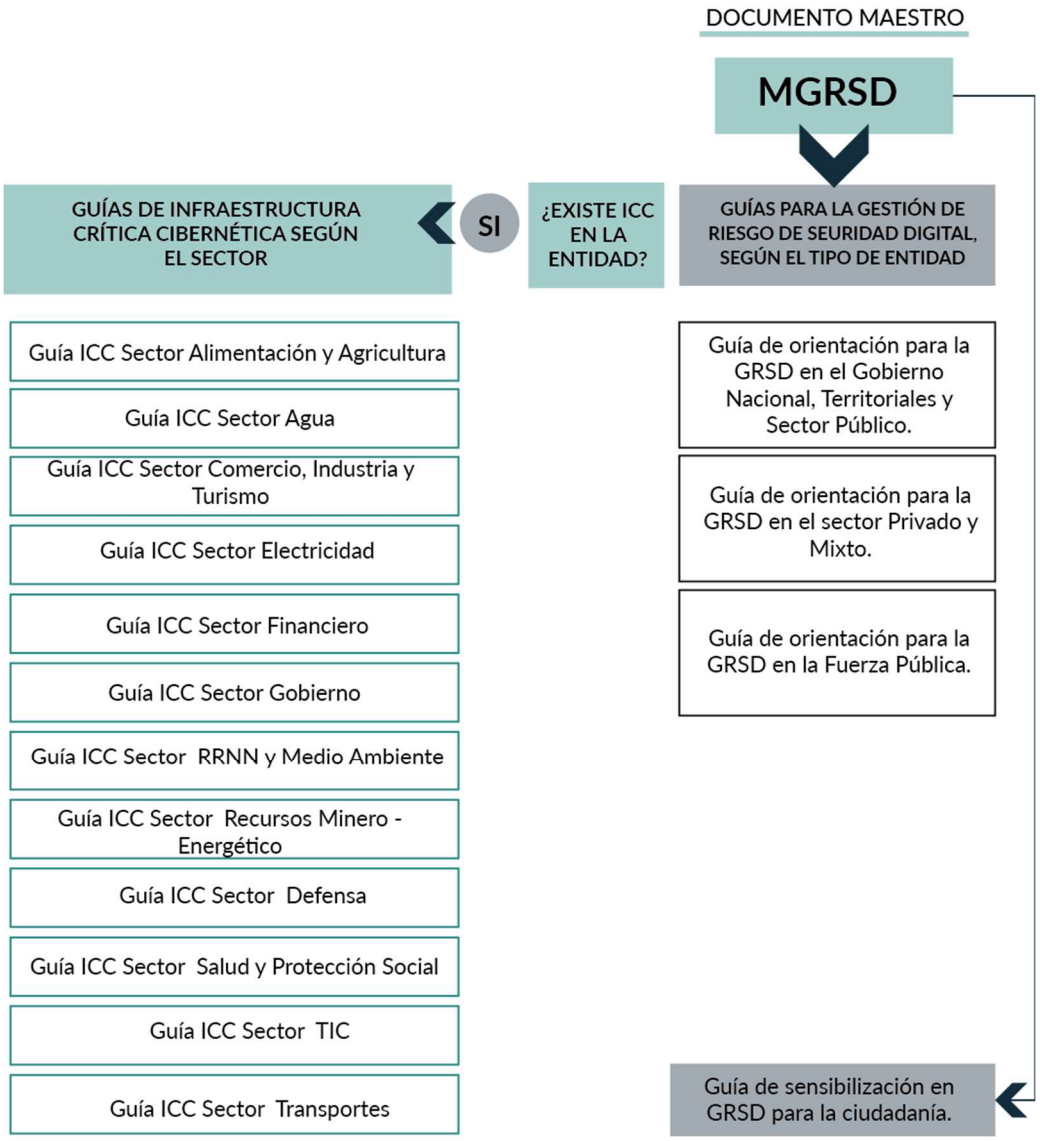

Ilustración 3 Modelo nacional de gestión de riesgos de seguridad digital

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.

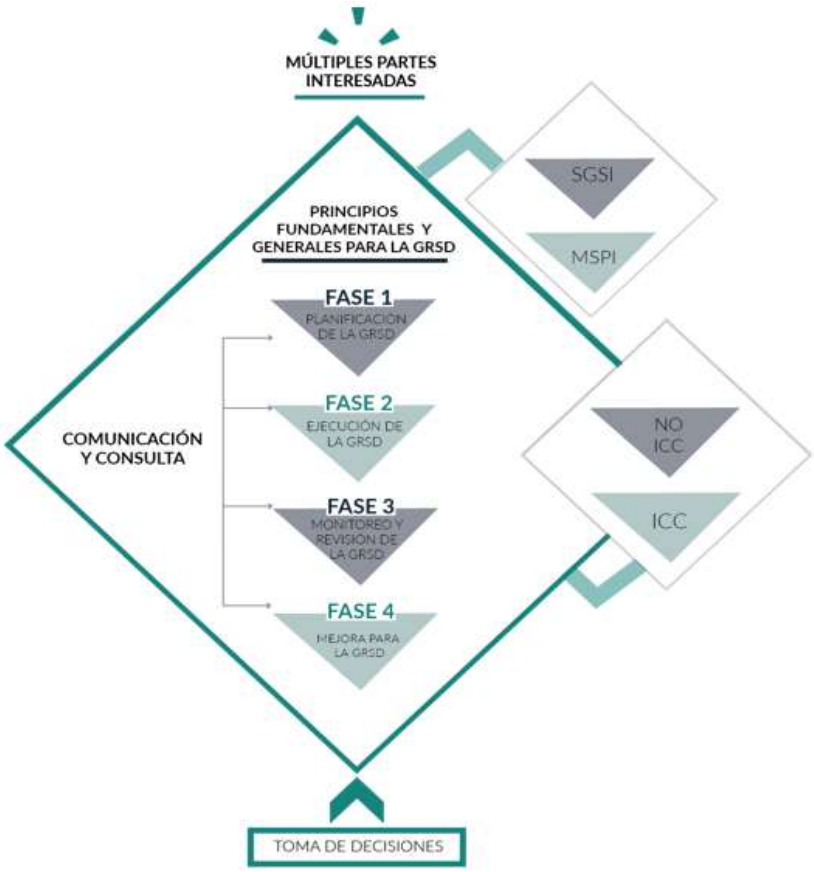

Ilustración 4 Fase modelo nacional de gestión de riesgos de seguridad digital

9 POLÍTICA Y LINEAMIENTOS DE GESTIÓN DEL RIESGO EN EL FONDO 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/15RjZBzZPUgHOwGUIr2DqCIfa7ZlbX746/view?usp=sharing

10 ACTIVIDADES 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.

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.

12 ANEXOS

Anexo 1 Cronograma actividades

ANEXO 1. CRONOGRAMA DE ACTIVIDADES FONDO ADAPTACIÓN

Ítem	Gestión / Proyecto	Actividades	Responsables	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
1	Gestión de Riesgos	Realizar identificación, valoración y definición de plan de tratamiento anual de los riesgos de seguridad.	Profesional de Seguridad de la Información	Jun-23	Jul-26
2	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 anual	Profesional de Seguridad de la Información	Mar-23	Dic-26
3	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	Feb-23	Dic-26
4	Implementación de controles	Renovación de herramientas de seguridad adquiridas	Profesional de Seguridad de la Información	Mar-23	Dic-26
		Adquisición anual de pruebas de ingeniería social	Proveedor o tercero		
		Adquisición de campañas de sensibilización	Profesional de Seguridad de la Información Proveedor o tercero		
		Adquisición y configuración de herramienta de gestión del SGSI.	Profesional de Seguridad de la Información Proveedor o tercero		
		Ejecutar Pruebas de Seguridad tipo Análisis de Vulnerabilidades.	Proveedor o tercero		
		Diseñar e implementar los controles de seguridad.	Profesional de Seguridad de la Información.		
		Elaborar plan de mejoramiento	Control Interno Profesional de Seguridad de la		
5	Indicadores SGSI	Definición, revisión y evaluación de los indicadores de medición del SGSI semestralmente.	Profesional de Seguridad de la Información	Ene-23	Dic-26

Ilustración 5 Cronograma