COLOMBIA POTENCIA DE LA VIDA

Fondo Adaptación

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2023-2026

Versión 00, 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 SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023-2026.

Versión 0.0, enero 2024, Bogotá D.C.

CONTROL DE CAMBIOS Y NOMENCLATURA

VERSIÓN	FECHA	DESCRIPCIÓN
1.0	2023/01	Documento Inicial
1.1	2023/02	Documento Ajustado alcance y marco legal
2.0	2023/05	Documento Ajustado alcance, objetivos
0.0	2024/01	Borrador Actualización según lineamientos planeación 2024, revisión de cronograma 2024

Tabla de Contenido

Tablas

Ilustraciones

1 INTRODUCCIÓN

Con la evolución de los ataques informáticos y los avances tecnológicos, se ve la necesidad de establecer e implementar directivas y controles que permitan el aseguramiento de la información y proteger sus criterios de confidencialidad, integridad y disponibilidad de la misma, es así como a nivel gubernamental se define el Modelo de Seguridad y Privacidad de la Información (MSPI), el cual cuenta con diferentes fases, donde se establece el diagnóstico, planeación, implementación, verificación y actuar, con el din de asegurar la información.

Dentro del Modelo de Seguridad y Privacidad de la Información, se contemplan grandes conjuntos de actividades que se desarrollan 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.

De acuerdo con lo anterior se desarrollan planes que se enfocan en las actividades que realizará el FONDO para la implementación de dicho Modelo y así fortalecer la seguridad de la información.

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 Plan de Seguridad y Privacidad de la Información de la entidad toma como referencia el Modelo de Seguridad y Privacidad de la Información (MSPI), emitido por el Ministerio de las TIC como órgano regulador en la materia.

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

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

Es importante mencionar que la Entidad tiene una Política de Seguridad de la Información desde el año 2014 y que ha venido siendo actualizada cada año. Esta política puede ser consultada en el siguiente vínculo:

https://www.fondoadaptacion.gov.co/index.php/politica-de-seguridad-sgsi.html

4 ANÁLISIS DE CONTEXTO

En esta sección se realiza un entendimiento de la situación actual de la entidad en términos de Seguridad de la información y la relación con el FURAG.

4.1 Seguridad y Privacidad de la Información

En materia de seguridad de la información, y de acuerdo con el autodiagnóstico realizado en la vigencia 2023, se observan avances representativos en materia de Seguridad y Privacidad de la Información.

La implementación del Modelo de Seguridad y Privacidad de la Información se realiza con base en las directrices y lineamientos del Ministerio de tecnologías de la Información y como soporte de ello, se inician las actividades con la definición de las políticas de seguridad de la información, identificando partes internas y externas y lo roles y responsabilidades.

5 AVANCES

- Durante la implementación del Modelo de Seguridad de la Información – MSPI se han realizado las siguientes actividades:

- Se elabora la política general y manual de políticas de seguridad y privacidad de la información.

- Se inicia la transición de IPv4 a IPV6 en los servicios de nube, los cuales ya tienen una implementación inicial.
- Se cuenta con la metodología de gestión de activos de información donde se incluyen los aspectos de cumplimiento legal, fechas de actualización, propietarios y criticidad de los activos.
- Se realiza el plan de sensibilización y capacitación en seguridad de la información.
- Realizar identificación y socialización de riesgos de seguridad en todos los procesos de la Entidad.
- Se realiza gestión de riesgos, partiendo de los activos de información identificados.
- Se tienen definidos ANS sobre los servicios que se prestan a los usuarios
- Se envían tips de seguridad y se realiza capacitación en seguridad de la información.
- Se han definido las capacidades actuales y futuras de los servicios tecnológicos.
- Se tiene un procedimiento formal para atender los requerimientos de soporte.
- Se tiene un catálogo de servicios tecnológicos parcialmente actualizado.
- La infraestructura tecnológica de la entidad: computadores, licenciamiento ofimático cumple con las necesidades actuales.
- Existe estrategia de uso y apropiación que incluye una matriz de los grupos de interés, un catálogo de entrenamiento y un plan de gestión del cambio.

5.1 Problemáticas

De acuerdo con el análisis del entendimiento estratégico y la madurez tecnológica de la entidad y el Modelo de Seguridad y Privacidad de la Información en cada uno de sus dominios, así como el modelo operativo de Tecnología, se pueden identificar las siguientes problemáticas:

ID	Descripción	Dominio
1	El área de TI no participa con voz y voto en el comité directivo.	Gobierno de TI
2	No se tiene una evaluación y proyección de las capacidades de TI en términos de personas, procesos y tecnología. En este momento los recursos son insuficientes para atender las necesidades de TI de la entidad.	Gobierno de TI
3	No se tiene una metodología formal para la gestión de proyectos de TI documentada.	Gobierno de TI
4	El área de TI se considera un área operativa más no estratégica.	Gobierno de TI
5	No se han identificado datos maestros y no existe un esquema de gobierno y de gestión de los componentes de información donde se gestione la calidad de estos.	Gestión de Información
6	No existe una metodología de referencia para el desarrollo de los sistemas de información, como tampoco se cuenta con estándares o lineamientos claros para la implementación de sistemas de información.	Sistemas de Información
7	No está documentada la arquitectura de solución y referencia de los sistemas de información.	Sistemas de Información
8	No existe un plan de aseguramiento de calidad de los sistemas de información	Sistemas de Información
9	No existen planes de mantenimiento preventivo y evolutivo sobre toda la infraestructura y demás servicios tecnológicos	Servicios Tecnológicos
10	Finalizar la implementación del protocolo IPV6, por lo que es necesario ajustar los servicios tecnológicos para que quede operativo.	Servicios Tecnológicos
11	Falta culminar la implementación del Modelo de Seguridad y Privacidad de la Información – SSPI de acuerdo con el Modelo de MINTIC - MSPI	Seguridad y Privacidad
12	Culminar la identificación, clasificación y calificación de los activos tipo	Seguridad y

ID	Descripción	Dominio
	software, hardware, servicios y personas.	Privacidad
13	Falta incluir dentro del Plan Anual de Capacitación Institucional las Capacitaciones en Seguridad de la Información.	Seguridad y Privacidad
14	Falta formalización de formatos para la gestión de incidentes de seguridad de la información y los derivados del Modelo de Seguridad y privacidad de la Información.	Seguridad y Privacidad
15	Fortalecer las capacidades institucionales en el manejo de la política de seguridad y privacidad de la información.	Seguridad y Privacidad
16	Falta presentar al comité Institucional de Gestión y Desempeño el alcance de seguridad para implementar el Sistema de Gestión de Seguridad de la Información.	Seguridad y Privacidad
17	No se cuenta con un plan de continuidad operativa.	Seguridad y Privacidad Servicios tecnológicos

Tabla 1 Problemáticas

5.2 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.

.

6 OBJETIVOS

6.1 Objetivo General

Proveer un Plan de Seguridad y Privacidad de la Información de la Entidad para definir la hoja de ruta de la estrategia de ciberseguridad, mediante la aplicación del habilitador de seguridad de la información de la política de gobierno digital, con el fin de proteger y preservar la confidencialidad, integridad y disponibilidad de la información de la Entidad.

6.2 Objetivos estratégicos

- Implementar y proteger los activos de información del Fondo Adaptación, con base en los principios de confidencialidad, integridad y disponibilidad.
- Gestionar los riesgos de seguridad de la información para mantenerlos en niveles aceptables.
- Sensibilizar a los servidores públicos y contratistas de la Entidad en Seguridad de la Información, fortaleciendo el nivel de conciencia de estos, en cuanto a la necesidad de salvaguardar los activos de información críticos de la Entidad.

- Monitorear el cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico.
- Implementar acciones correctivas y de mejora para del Modelo de Seguridad y Privacidad de la Información de Gobierno Digital".
- Gestionar los incidentes de seguridad de la información, con el fin de prevenir el impacto negativo para la Entidad. En cuanto pérdidas económicas, sanciones disciplinarias, legales, entre otras.

7 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 la implementación y mantenimiento del Modelo de Seguridad y Privacidad de la Información, 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.

La Alta Dirección designará un representante ante el Modelo de Seguridad y Privacidad 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.

8 MARCO NORMATIVO

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

8.1 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)”

8.2 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.

9 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 Modelo de Seguridad y Privacidad de la Información brindado confianza y seguridad a las partes interesadas.

Ilustración 1 Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

Fuente: E.T. Tecnologías de la Información

10 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 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	Implementación 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	Feb-23	Feb-26
2	Políticas de Seguridad de la Información	Revisión y actualización anual del Manual y Resolución de Políticas de Seguridad de la Información.	Profesional de Seguridad de la Información	Mar-23	Abr-26
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	Abr-23	Jun-26
		Realiza identificación y actualización anual de los Activos de Información.	Profesional de Seguridad de la Información		
		Socialización de activos de información anual	Profesional de Seguridad de la Información		
		Realizar clasificación anual de los activos de información.	Profesional de Seguridad de la Información		
4	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
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	May-23	Dic-26
		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 información anual	Profesional de Seguridad de la Información	Mar-23	Dic-26
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	Feb-23	Dic-26
8	Continuidad de las Operaciones	Definir o actualizar anualmente el plan de continuidad de las operaciones.	Profesional de Seguridad de la Información	May-24	Jul-26
		Diseñar y gestionar las pruebas al plan de continuidad de las operaciones.	Profesional de Seguridad de la Información Profesional de Infraestructura.	Ago-24	Nov-26
		Documentar las pruebas realizadas.	Profesional de Seguridad de la Información		
9	Protección de Datos Personales	Revisar y actualizar anualmente la política de Protección de	Responsable de Protección de Datos Personales.	Abr-24	Ago-26

		Datos Personales.	Profesional de Seguridad de la Información		
10	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.		
11	Auditorías	Ejecución de Auditoría Interna anual al SGSI	Control Interno	Nov-24	Dic-26
		Elaborar plan de mejoramiento	Control Interno Profesional de Seguridad de la		
12	Indicadores SGSI	Definición, revisión y evaluación de los indicadores de medición del SGSI semestralmente.	Profesional de Seguridad de la Información	Ene-23	Dic-26
13	Certificación ISO 27001:2022	Realizar revisiones de los procesos que se van a postular para la certificación.	Profesional de Seguridad de la Información	Ene-24	Dic-26
		Realizar diagnóstico de los procesos seleccionados	Profesional de Seguridad de la Información		
		Aplicar las acciones de mejora.	Profesional de Seguridad de la Información Proceso de la Entidad		
		Elaborar y/o actualizar la documentación requerida para la certificación.	Profesional de Seguridad de la Información Proceso de la Entidad		
14	Solicitud de otorgamiento de certificación ISO 27001:2022	Realizar la gestión y atender la auditoría de otorgamiento del certificado de la Norma ISO 27001:2022	Control Interno Profesional de Seguridad de la Información	mar-26	oct-26

Tabla 2 Cronograma