Ambiente

Plan de Seguridad y Privacidad de la Información - 2025

Proceso

Gestión Estratégica de Tecnologías de la Información

Versión 3

30/01/2025

TABLA DE CONTENIDO

1. INTRODUCCIÓN 3
2. OBJETIVO GENERAL 4
3. OBJETIVOS ESPECÍFICOS 4
4. ALCANCE 5
5. DEFINICIONES 5
6. MARCO LEGAL 6
7. ESTADO ACTUAL 7
8. IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD 10

TABLA DE TABLAS

Tabla 6.1 Marco Normativo 7
Tabla 7.1 Evaluación de los controles 10
Tabla 8.1 Cronograma de actividades 13

1. INTRODUCCIÓN

El Ministerio de Ambiente y Desarrollo Sostenible en la resolución 2140 del 19 de octubre de 2017, "*Por la cual se adopta el Modelo Integrado de Planeación y Gestión y se crean algunas instancias administrativas al interior del Ministerio de Ambiente y Desarrollo Sostenible y se dictan otras disposiciones*", constituye el comité institucional de gestión y desempeño para "*Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información impartidas por la Presidencia de la Republica y el Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC*", establece la planificación e implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) mediante el desarrollo de políticas de gestión y desempeño alineadas con las necesidades, requisitos de seguridad y los objetivos estratégicos del Ministerio.

Para gestionar el Modelo de Seguridad y Privacidad de la Información, el Ministerio de Ambiente y Desarrollo Sostenible reconoce la importancia de proteger su activo más valioso como lo es la información generada o transformada. Por ello requiere continuar y alcanzar un nivel de madurez óptimo en el Sistema de Gestión de Seguridad de la Información-SGSI, preservando la confidencialidad, integridad, y disponibilidad de la información, enmarcado en el cumplimiento de la legislación, políticas y lineamientos relacionados con la gestión, administración y protección de la información, aplicables a las entidades estatales, con un enfoque en el fortalecimiento de la información.

Este documento relaciona la información detallada necesaria para implementar y mantener la Seguridad de la Información del Ministerio para la vigencia 2025, estableciendo los requerimientos para garantizar el cumplimiento de los resultados esperados. Cabe destacar que, en 2024 se obtuvieron resultados significativos gracias a la ejecución de las acciones del Plan de Seguridad y Privacidad de la Información, entre las cuales se resaltan las siguientes:

- Se actualizó la metodología para la identificación y clasificación de los activos de información y los riesgos de seguridad de la información, lo que permitió mejorar la matriz de riesgos de seguridad. Esta actualización incluyó avances significativos en la implementación y el seguimiento de los controles establecidos por la norma ISO 27001.
- Actualización del registro de activos de información y de la matriz de riesgos de seguridad de la información, en coordinación con los procesos del Ministerio.
- Actualización y registro de las bases de datos personales ante la Superintendencia de Industria y Comercio.
- Se llevó a cabo la actualización de los siguientes documentos: Manual de Políticas Específicas de Seguridad, Declaración de Aplicabilidad (SoA) y la evaluación del instrumento del Modelo de Seguridad y Privacidad de la Información (MSPI). Fortalecimiento de la apropiación y

cultura institucional respecto a la Seguridad de la Información, procedimiento gestión de incidentes de seguridad de la información y vulnerabilidades.

2. OBJETIVO GENERAL

Definir la hoja de ruta para el fortalecimiento del Sistema de Gestión de Seguridad de la Información del Ministerio de Ambiente y Desarrollo Sostenible durante la vigencia 2025, esto incluye la planificación de actividades estratégicas orientadas a la mejora continua, el fortalecimiento de la protección y preservación de la confidencialidad, integridad y confidencialidad de la información institucional. Dichas acciones se fundamentarán en los lineamientos del Modelo de Seguridad y Privacidad de la Información, alineados con la NTC/IEC ISO 27001, el Manual de Políticas de Seguridad de la Información, la Política General de Seguridad de la Información, las recomendaciones del FURAG para la implementación de la Política de Seguridad Digital y los lineamientos del Modelo Integrado de Planeación y Gestión – MIPG.

3. OBJETIVOS ESPECÍFICOS

- Gestionar las diferentes acciones para la mejora continua y apropiación del Sistema de Gestión de Seguridad de la Información, con el objetivo de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información del Ministerio.
- Fortalecer el nivel de madurez del Modelo de Seguridad y Privacidad de la Información en el Ministerio.
- Gestionar los riesgos de seguridad de la información con el liderazgo de los procesos del Ministerio, que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información.
- Sensibilizar a los servidores públicos (funcionarios y contratistas) del Ministerio sobre el Sistema de Gestión de Seguridad de la Información (SGSI), fomentando una cultura institucional centrada en la protección de la información, así como socializar y difundir buenas prácticas y recomendaciones en materia de seguridad.

4. ALCANCE

Este documento es aplicable a todos los niveles del Ministerio, a sus funcionarios, contratistas y personas o terceros que, por cumplimiento de sus obligaciones, funciones y del Ministerio, compartan, utilicen, recolecten, procesen, intercambien o consulten su información, y a los entes de control, entidades relacionadas que accedan interna o externamente a cualquier activo de información, independientemente de su ubicación. Este plan aplica a toda la información creada, procesada o utilizada por el Ministerio, sin importar el medio, formato o presentación o lugar donde se encuentre.

5. DEFINICIONES

Activos: Todo aquello que es de valor para la organización.

Activos de información: Datos y conocimiento de valor para la organización.

Confidencialidad: Propiedad mediante la cual la información no se hace disponible o revelada a individuos, procesos o entidades no autorizadas.
Dato Personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (Ley 1581/2012).

Integridad: Propiedad de protección de la exactitud y completitud de la información.

Control: Medio para gestionar el riesgo (Políticas, procedimientos, guías, practicas o estructuras).

CSIRT: Equipo de respuesta a incidentes cibernéticos del país.

Disponibilidad: propiedad que permite que la información siempre esté accesible y utilizable para las personas autorizadas. En otras palabras, hace referencia a mantener activo el acceso a la información necesaria en el momento que sea necesario.

MSPI: Modelo de Seguridad y Privacidad de la Información.

SGSI: Sistema de Gestión de Seguridad de la Información.

OTIC: Oficina de Tecnologías de la Información y las Comunicaciones del Ministerio de Ambiente y Desarrollo Sostenible.

Riesgo: Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen institucional, entre otro.) y se pueden aplicar a niveles diferentes (operativo, estratégico, organización).

Seguridad de la Información: Todas las acciones orientadas a preservar la integridad, confidencialidad y disponibilidad de la información y los activos asociados a su tratamiento, independiente de la forma en la que se encuentren.

Sensibilización: Es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.

6. MARCO LEGAL

El Plan de Seguridad y Privacidad de la Información de la vigencia 2025 del Ministerio, se encuentra definido teniendo en cuenta el siguiente marco normativo.

MARCO LEGAL	FECHA	CONTEXTO
Directiva Presidencial 02	Febrero 24 de 2022	"Para garantizar la implementación segura de la Política de Gobierno Digital liderada por el Ministerio de Tecnologías de la Información y las comunicaciones (MinTIC)".
Decreto 338	Marzo 8 de 2022	"Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones".
Resolución 746	Marzo 11 de 2022	"Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021".
Decreto 767	Mayo 16 de 2022	"Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
Resolución 500	Marzo 10 de 2021	"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital".

MARCO LEGAL	FECHA	CONTEXTO
Resolución 1519	Agosto 24 de 2020	"Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos".
Resolución 2140	Octubre 19 de 2017	"Por la cual adopta el Modelo Integrado de Planeación y Gestión y se crean algunas instancias administrativas al interior del Ministerio de Ambiente y Desarrollo Sostenible y del Fondo Nacional Ambiental, y se dictan otras disposiciones".
Conpes 3854	Abril 11 de 2016	Política Nacional de Seguridad Digital. Busca fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia.
Decreto 103 de 2015	Enero 20 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Ley 1712	Marzo 06 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 1377	Junio 23 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Ley 1581	Octubre 17 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013.

Tabla 6.1 Marco Normativo

7. ESTADO ACTUAL

El Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC elaboró el Modelo de Seguridad y Privacidad de la Información - MSPI y define los lineamientos para la implementación de la estrategia de seguridad digital, con el objetivo de formalizar al interior de las entidades públicas un Sistema de Gestión de Seguridad de la Información - SGSI y Seguridad Digital, el cual contempla su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento; el modelo consta de cinco (5) fases las cuales permiten que las Entidades puedan gestionar y mantener adecuadamente la seguridad y privacidad de cada uno de los procesos, trámites, servicios, sistemas de información, infraestructura

y, en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de la información, a continuación se detallan las cinco fases a implementar:

- **Diagnóstico:** Evaluar el estado actual de la seguridad y privacidad de la información en el Ministerio. Esto incluye la identificación de riesgos, brechas, y niveles de cumplimiento frente a la normatividad y controles de seguridad.
- **Planificación:** Determinar las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo.
- **Operación:** Ejecutar las estrategias y controles de seguridad de la información previamente planificados. Esta fase incluye la adopción de medidas técnicas y administrativas, capacitación al personal, y el despliegue de herramientas y tecnologías necesarias.
- **Evaluación de Desempeño:** Seguimiento continuo de la implementación del MSPI mediante indicadores y auditorías internas, asegurando que los controles estén operando de manera efectiva y se mantenga la seguridad y privacidad de la información.
- **Mejoramiento Continuo:** Establecer procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición.

Ciclo de Operación del Modelo de Seguridad y Privacidad de la Información, Fuente: "Modelo de Seguridad y Privacidad de la Información" - Anexo 1 de la Resolución 500 de 2021 de MinTIC.

De acuerdo con lo anterior, el Ministerio establece, actualiza, aprueba, publica y divulga documentos estratégicos como el Plan de Seguridad y Privacidad de la Información, la Política General de Seguridad de la Información, el Plan de Tratamiento de Riesgos de Seguridad de la Información y otros relacionados con el Sistema de Gestión de Seguridad de la Información (SGSI). A través de estos, se definen las estrategias, controles y acciones necesarias para gestionar de manera integral la seguridad y privacidad de la información en todos los activos de información de la entidad. Estas medidas están orientadas a proteger la confidencialidad, integridad y disponibilidad de la información, mitigar los riesgos asociados a la seguridad y privacidad de los datos, asegurar el cumplimiento de las normativas vigentes y garantizar la continuidad de los procesos institucionales ante posibles amenazas o vulnerabilidades.

Durante el transcurso de la vigencia 2024, se realizó la evaluación del Modelo de Seguridad y Privacidad de la Información, ésta se realiza con la aplicación del "instrumento Evaluación MSPI del MINTIC", el cual permite determinar el estado actual de la gestión de seguridad y privacidad de la información en el Ministerio.

La evaluación del Modelo consiste en la valoración de los diferentes controles administrativos y técnicos que componen la ISO 27001:2013, identificando las brechas, los soportes documentales de cumplimiento de cada control ISO y la formulación de actividades para la mejora continua en la implementación del MSPI en toda la Entidad, el cual se soporta en el modelo de operación PHVA (Planear, Hacer, Verificar, Actuar), con un enfoque en la valoración de los diferentes dominios con sus respectivos controles administrativos y técnicos de la norma ISO 27001:2013, identificando brechas, recopilando los soportes documentales que demuestran el cumplimiento de cada control, y formulando actividades para la mejora continua en la implementación del MSPI.
A continuación, se muestra el resultado de la implementación de los controles evaluados en el MSPI al 2024:

Resultado de evaluación de los controles

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	64	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	71	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	65	100	GESTIONADO
A.9	CONTROL DE ACCESO	60	100	EFECTIVO
A.10	CRIPTOGRAFÍA	70	100	GESTIONADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	70	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	73	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	65	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	60	100	EFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	70	100	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	60	100	EFECTIVO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	57	100	EFECTIVO
A.18	CUMPLIMIENTO	74	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		67	100	GESTIONADO

Tabla 7.1 Evaluación de los controles

El resultado de la evaluación de los controles fue satisfactorio, ya que de los catorce (14) dominios evaluados, once (11) se encuentran en la escala de "Gestionado" y tres (3) en "Efectivo". En promedio, la evaluación de los controles arrojó un puntaje de 67 sobre 100.

8. IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD

La etapa de implementación del Plan de Seguridad y Privacidad de la Información para la vigencia 2025 del Ministerio, se centra en el análisis, ejecución y cumplimiento de las actividades y objetivos planeados, teniendo en cuenta los roles y responsabilidades y los tiempos de cumplimiento por parte del equipo de trabajo involucrado (todos los procesos, actores clave, colaboradores, equipo directivo, partes interesadas, entre otros). El resultado esperado de esta fase es la adecuada implementación y cumplimiento de las actividades previstas en el presente documento.

El Plan de Seguridad de la Información comprende el siguiente cronograma de actividades con sus correspondientes responsables, fecha de inicio y fecha de finalización:

COMPONENTE	ACTIVIDAD	TAREAS	EVIDENCIAS	RESPONSABLE	DURACIÓN (MES)	
					Inicio	Fin
Plan de Seguridad y Privacidad de la Información y Plan de Tratamiento de Riesgos	Revisión y actualización del Plan de Seguridad y Privacidad de la Información.	Revisar y actualizar el Plan de Seguridad y Privacidad de la Información.	Reunión para revisar y actualizar	Equipo de seguridad.	Diciembre 2024	Diciembre 2024
	Aprobación del Plan de Seguridad y Privacidad de la Información por el CIGD.	Socializar ante el CIGD para aprobación del Plan de Seguridad y Privacidad de la Información.	Acta del comité o Presentación (ppt) de temas al comité en dónde fue aprobado.	CIGD/OAP	Diciembre 2024	Diciembre 2024
	Publicación del Plan de Seguridad y Privacidad de la Información.	Publicar en la página web, el Plan de Seguridad y Privacidad de la Información.	Plan actualizado en SOMOSIG y Página Web.	Equipo de seguridad /Comunicaciones	Enero 2025	Enero 2025
Registro Nacional de Bases de Datos Personales- RNBD	Registro de las bases de datos	Registrar las bases de datos teniendo en cuenta la información suministrada por las dependencias de los activos de información.	Certificado RNBD que expide la SIC	Equipo de Seguridad	Febrero 2025	Marzo 2025
Activos de Información	Actualización activos de información.	Gestionar el proceso de actualización de los activos de información con los procesos del Ministerio.	Activos de información actualizados en el formato institucional.	Procesos/Equipo de seguridad	Cuando se requiera	Cuando se requiera
	Consolidación de los activos de información de	Consolidar los activos de información de	Registro de activos de información.	Equipo de seguridad	Cuando se requiera	Cuando se requiera

COMPONENTE	ACTIVIDAD	TAREAS	EVIDENCIAS	RESPONSABLE	DURACIÓN (MES)	
					Inicio	Fin
	las dependencias.	las dependencias.				
	Aprobación activos de información.	Socializar ante el CIGD para aprobación los activos de información.	Acta del comité o Presentación (ppt) de temas al comité en dónde fue aprobado.	CIGD/OAP	Cuando se requiera	Cuando se requiera
	Publicación del registro de activos de información.	Publicar en la página web, el registro de activos de información.	URL de publicación.	UCGA/Equipo de seguridad	Cuando se requiera	Cuando se requiera
Gestión de Riesgos de Seguridad de la Información	Actualización riesgos de seguridad de la Información.	Gestionar el proceso de actualización de los riesgos de seguridad de la información a partir de los activos de información de los procesos del Ministerio.	Mapa de riesgos de SI actualizados.	Equipo de Seguridad OAP y Procesos	Cuando se requiera	Cuando se requiera
	Consolidación de los riesgos de seguridad de la información de los procesos.	Consolidar los riesgos de seguridad de la información dependencias.	Mapa de riesgos consolidados.	Equipo de seguridad.	Cuando se requiera	Cuando se requiera
	Aprobación Riesgos de SI.	Gestionar la aprobación de los riesgos de SI.	Acta del comité o Presentación (ppt) de temas al comité en dónde fue aprobado.	OAP/Equipo de seguridad	Cuando se requiera	Cuando se requiera
Gestión de Incidentes de	Incidentes de Seguridad de la Información gestionados	Gestionar los incidentes de seguridad de la información reportados a la	Casos de soporte gestionados de los incidentes de SI	Equipo de Seguridad	Cuando se requiera	Cuando se requiera

COMPONENTE	ACTIVIDAD	TAREAS	EVIDENCIAS	RESPONSABLE	DURACIÓN (MES)	
					Inicio	Fin
Seguridad de la Información		mesa de asistencia.				
Gestión de vulnerabilidades de Seguridad	Vulnerabilidades de seguridad	Gestionar las vulnerabilidades de seguridad de la información reportados a la mesa de asistencia y al plan de trabajo de análisis de vulnerabilidades (Cronograma de Excel)	Casos de soporte gestionados de las vulnerabilidades.	Equipo de Seguridad	Enero 2025	Diciembre 2025
Documentación SGSI	Formulación y/o actualización de la documentación del SGSI	Formular y/o actualizar la documentación de seguridad de la información.	Documentación publicada en SOMOSIG	Equipo de Seguridad	Cuando se requiera	Cuando se requiera

Tabla 8.1 Cronograma de actividades.