Ambiente

Plan de Seguridad y Privacidad de la Información - 2026

Proceso

Gestión Estratégica de Tecnologías de la Información

Versión 4

28/01/2026

Tabla de contenido

Tabla de tablas.

1. INTRODUCCIÓN

El Ministerio de Ambiente y Desarrollo Sostenible, mediante 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", establece el Comité Institucional de Gestión y Desempeño como la instancia responsable de asegurar la implementación y el desarrollo de las políticas de gestión y las directrices en materia de seguridad digital y seguridad de la información, emitidas por la Presidencia de la República y el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.

Asimismo, dicha resolución dispone la planificación e implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), mediante el desarrollo de políticas, lineamientos y prácticas alineadas con las necesidades institucionales, los requisitos de seguridad y los objetivos estratégicos del Ministerio.

En el contexto actual, donde la información constituye uno de los activos más críticos para las entidades, la seguridad de la información se establece como un pilar fundamental para garantizar su confidencialidad, integridad, disponibilidad y privacidad. En este marco, el Plan de Seguridad y Privacidad de la Información se formula con el propósito de proporcionar un marco integral, articulado y sistemático que permita al Ministerio proteger de manera eficaz la información sensible y los activos de información frente a amenazas internas y externas, así como frente a riesgos operativos, en el marco del Sistema de Gestión de Seguridad de la Información (SGSI).

La innovación de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de los procesos misionales, estratégicos y de apoyo, exige una atención prioritaria a la protección de la información. En consecuencia, el presente plan se diseña para alinear las iniciativas de seguridad con los objetivos estratégicos del Ministerio, asegurando que las medidas de protección implementadas no solo reduzcan los riesgos, sino que además fortalezcan la confianza de los ciudadanos, los grupos de interés y las partes interesadas en la gestión y prestación de servicios institucionales.

Este documento establece las directrices y acciones estratégicas que se implementarán en el horizonte del próximo cuatrienio, en consonancia con el Plan Nacional de Desarrollo vigente a partir de 2026, con el fin de:

a) **Fortalecimiento de la cultura de seguridad**: Impulsar una cultura institucional que promueva la práctica responsable y consciente de la seguridad de la información en todos los niveles de la Entidad.
b) **Gestión de riesgos:** Identificar, analizar, evaluar y tratar los riesgos relacionados con la seguridad de la información de manera proactiva, conforme a metodologías y mejores prácticas nacionales.
c) **Cumplimiento normativo:** Asegurar la observancia de las leyes, regulaciones, estándares y

lineamientos que rigen la seguridad de la información y la protección de datos personales.

d) **Capacitación y concienciación:** Desarrollar programas de formación y sensibilización continua para los servidores, contratistas y demás partes interesadas, con el fin de reducir la probabilidad de incidentes ocasionados por el factor humano.
e) **Protección de activos**: Implementar controles físicos, lógicos, administrativos y tecnológicos que permitan salvaguardar los activos de información frente a accesos no autorizados, pérdidas, divulgación indebida o daños.
f) **Respuesta a incidentes:** Establecer procedimientos claros, oportunos y eficaces para la detección, análisis, tratamiento y recuperación ante incidentes de seguridad, con el fin de minimizar su impacto operativo, reputacional y jurídico.

La actualización del Plan de Seguridad y Privacidad de la Información a la versión de la norma ISO 27001:2022 es esencial para adaptarse a los cambios tecnológicos, las amenazas emergentes y las regulaciones actuales. Esto no solo permite asegurar el cumplimiento con las nuevas normativas, sino que también mejora la gestión de riesgos, fortalece la resiliencia organizacional, y optimiza la seguridad de la información del Ministerio. La actualización permite mantener un enfoque proactivo, eficiente y alineado con las mejores prácticas en seguridad, ciberseguridad y privacidad de la información, lo cual es crucial para proteger la información valiosa y garantizar la continuidad operativa del Ministerio.

2. MARCO NORMATIVO

El Plan de Seguridad y Privacidad de la Información se basa en los documentos, normas y lineamientos para su estructura y funcionamiento que se relacionan a continuación:

Tabla 1 Marco Normativo Aplicable

Marco Normativo	Descripción
Ley Estatutaria 1266 de 2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos.
Ley 2012 Estatutaria 1581 de	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 2609 de 2012	Por el cual se reglamenta el Título V de la Ley 594 de 2000 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".

Marco Normativo	Descripción
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Ley 1712 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 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de2014 y se dictan otras disposiciones
Decreto 1078 de 2015	Modificado por el Decreto 1008 de 2018 - Política de Gobierno Digital que contiene el Modelo de seguridad y Privacidad - MSPI de MINTIC.
CONPES 3854 de 2016	Política de Seguridad Digital del Estado Colombiano
Decreto 1499 de 2017	El cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión.
Ley 1928 de 2018	Por medio de la cual se aprueba el "Convenio sobre La Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest
Decreto 612 DE 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
CONPES 3854 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.
CONPES 3995 de 2020	Política Nacional De Confianza y Seguridad Digital
Resolución 1519 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 Materia de acceso a la Información pública, accesibilidad web, seguridad digital, y datos abiertos.
Resolución 746 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 500 de 2021.
Resolución 02277 de 2025 del Ministerio de Tecnologías de la Información y las Comunicaciones	Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.

3. DEFINICIONES

- **Activo**: 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 de seguridad de la información**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias
- **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.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Definir las actividades para incrementar el nivel de madurez de seguridad y privacidad de la Información en el Ministerio de Ambiente y Desarrollo Sostenible para la vigencia 2026, el estándar internacional ISO/IEC 27001:2022, estrategias de Gobierno Digital, MIPG, requerimientos de la entidad y disposiciones legales vigentes; con el fin de garantizar la confidencialidad, disponibilidad, integridad y privacidad de los activos de información del Ministerio.

4.2 OBJETIVOS ESPECIFICOS

- Definir, estructurar e implementar la estrategia de seguridad digital de la Entidad, alineada con los lineamientos del MSPI, del MIPG y con los objetivos estratégicos institucionales, para garantizar la protección integral de los activos de información.
- Identificar, documentar y priorizar las necesidades técnicas, administrativas y operativas requeridas para la implementación y fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI), incluyendo recursos, capacidades, infraestructura y competencias del talento humano.
- Priorizar y planificar las actividades, iniciativas y acciones de seguridad de la información necesarios para la adecuada implementación, mantenimiento y mejora continua del SGSI, considerando el nivel de riesgo, el impacto institucional y la disponibilidad presupuestal.
- Establecer un plan sistemático de evaluación y seguimiento del desempeño de los controles, políticas y lineamientos implementados, con el fin de medir su eficacia, identificar brechas, proponer mejoras y garantizar el cumplimiento normativo en materia de seguridad de la información.

5. ALCANCE

El presente plan inicia con la adopción, actualización y fortalecimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) definido por el Ministerio de las TIC, incluyendo la Política General de Seguridad de la Información, el manual de políticas específicas, los procedimientos, guías, manuales, entre otros que respaldan su implementación. Asimismo, abarca la definición, gestión y aplicación de los controles necesarios para garantizar la adecuada protección de los activos de información identificados y aprobados por los procesos de la Entidad.

Este plan es de aplicación para todos los servidores públicos, contratistas y terceros que administren, procesen, almacenen, consulten o accedan a información, sistemas de información, infraestructura tecnológica y demás activos definidos en el registro de activos de información vigente, independiente del medio, formato o tecnología utilizada.

6. IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD-OPERACIÓN

La etapa de implementación del Plan de Seguridad y Privacidad de la Información para la vigencia 2026 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, Alta Dirección,

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

Tabla 2 Cronograma de actividades 2026.

COMPONENTE	ACTIVIDAD	TAREAS	EVIDENCIAS	RESPONSABLE	INICIO	FIN
Transición a la nueva norma ISO 27001:2022 y preparación para la certificación	Realizar diagnóstico de cumplimiento de los requisitos y controles de la ISO 27001:2022	Realizar mesas de trabajo con las áreas responsables de controles para hacer el diagnóstico	Informe del diagnóstico sobre los requisitos y controles de la ISO 27001:2022	Equipo de seguridad.	Febrero 2026	Mayo 2026
	Elaborar y socializar el plan de trabajo para el cierre de brechas y la transición a la Norma ISO-IEC 27001:2022.	Socializar y aprobar el plan de cierre de brechas y transición.	Plan de cierre de brechas y transición a la norma ISO 27001:2022	Equipo de seguridad.	Junio 2026	Julio 2026
	Implementar el plan de trabajo de cierre de brechas y la transición a la Norma ISO-IEC 27001:2022	Seguimientos a la implementación del plan de trabajo	Soporte de ejecución de actividades del plan.	Equipo de seguridad	Julio 2026	Noviembre 2026
Mantenimiento del Programa de Protección de Datos Personales	Realizar diagnóstico del cumplimiento de Accountability	Realizar mesas de trabajo con las áreas internas responsables de bases de	Informe del diagnóstico de cumplimiento de la Ley 1581 de 2012	Equipo de Seguridad	Febrero 2026	Abril 2026

COMPONENTE	ACTIVIDAD	TAREAS	EVIDENCIAS	RESPONSABLE	INICIO	FIN
	de la Ley 1581 de 2012	datos con información personal				
	Actualizar inventario de bases de datos con información personal	Enviar memorando a todas las áreas del Ministerio para que reporten novedades en las bases de datos personales	Inventario de bases de datos personales actualizado	Equipo de Seguridad	Abril 2026	Junio 2026
	Actualizar la política de tratamiento y protección de datos personales	Ajustar el documento de la política según los requisitos del Decreto Reglamentario 1377 de 2013	Política de tratamiento y protección de datos personales actualizada y publicada en SomoSIG y el sitio web	Equipo de Seguridad	Junio 2026	Julio 2026
	Elaborar el Manual Interno de Políticas y Procedimientos de Datos Personales	Con base en el diagnóstico, elaborar el Manual Interno de Políticas y Procedimientos de Datos Personales según los requerimientos del Decreto Reglamentario 1377 de 2013	Manual Interno de Políticas y Procedimientos de Datos Personales publicado en SomoSIG	Equipo de Seguridad	Junio 2026	Agosto 2026
	Cierre de brechas del	Elaborar y ejecutar plan	Soportes de ejecución de	Equipo de	Abril 2026	Noviembre 2026

COMPONENTE	ACTIVIDAD	TAREAS	EVIDENCIAS	RESPONSABLE	INICIO	FIN
	diagnóstico de cumplimiento de la Ley 1581 de 2012	de cierre de brechas del cumplimiento de la Ley 1581 de 2012	actividades para el cierre de brechas	Seguridad		
	Actualizar el registro RNBD del MADS	Realizar la actualización del RNBD del MADS con todas las novedades presentadas durante la vigencia 2026	Certificación de actualización del RNBD con radicados.	Equipo de Seguridad	Noviembre2026	Diciembre 2026
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	Marzo 2026	Julio 2026
	Consolidación de los activos de información de las dependencias.	Consolidar los activos de información de las dependencias.	Registro de activos de información.	Equipo de seguridad	Agosto 2026	Octubre 2026
	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	Octubre 2026	Noviembre 2026
	Publicación del registro de	Publicar en la página web y en Datos	URL de publicación.	UCGA/Equipo de seguridad	Noviembre 2026	Diciembre 2026

COMPONENTE	ACTIVIDAD	TAREAS	EVIDENCIAS	RESPONSABLE	INICIO	FIN
	activos de información.	Abiertos el registro de activos de información.				
Gestión de vulnerabilidades de Seguridad	Vulnerabilidades de seguridad	Gestionar las vulnerabilidades de seguridad de la información reportados a la mesa de asistencia y al cronograma de análisis de vulnerabilidades (Cronograma de Excel)	Casos de soporte gestionados de las vulnerabilidades. Cronograma de vulnerabilidades 2026.	Responsable de SI	Enero 2026	Diciembre 2026

7. PRESUPUESTO

Los proyectos y recursos presupuestales destinados a seguridad perimetral y seguridad de la información para cada vigencia se encuentran definidos y programados en el Plan Anual de Adquisiciones de la Oficina de Tecnologías de la Información y la Comunicación.