



Agricultura

**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL MINISTERIO DE AGRICULTURA Y
DESARROLLO RURAL**



Agricultura



1. INTRODUCCIÓN

En el actual entorno digital, con una creciente dependencia en el entorno tecnológico de la información y una mayor importancia de la protección de la información y la privacidad, estos se considera que se convierten en elementos estratégicos necesarios para las entidades públicas en Colombia. La importancia de estos aspectos, esta relacionado con el cumplimiento que debe darse al marco normativo actual y a la preservación de la confianza de la ciudadanía de hacen parte de los pilares principales de la gestión pública.

El Plan de Seguridad y Privacidad de la Información del Ministerio de Agricultura y Desarrollo Rural, tiene como propósito establecer las directrices, estrategias y acciones necesarias para garantizar la protección de la confidencialidad, integridad y disponibilidad de los activos de información, en concordancia con las disposiciones legales y regulatorias aplicables en materia de seguridad digital, ciberseguridad y protección de datos personales, así como con las buenas prácticas y estándares internacionales, en particular la norma ISO/IEC 27001:2022. Adicionalmente, este plan promueve una gestión responsable y ética de los datos personales, alineada con los principios de transparencia, responsabilidad proactiva y respeto a los derechos de los titulares.

En concordancia con lo anterior, el Plan de Seguridad y Privacidad de la Información se formula en cumplimiento del Decreto 612 de 2018, el cual establece la integración de los planes institucionales al Plan de Acción Anual de las entidades del Estado. En este sentido, el presente Plan se articula con el Modelo Integrado de Planeación y Gestión –MIPG– y hace parte del proceso de planeación institucional del Ministerio de Agricultura y Desarrollo Rural para la vigencia 2026, permitiendo la planificación, ejecución y seguimiento de las acciones en materia de seguridad de la información y privacidad dentro del ciclo de gestión institucional.

La naturaleza de las funciones que lleva a cabo el Ministerio requiere proteger la información sensible, estratégica y los datos de carácter personal cuya afectación podría acarrear un efecto trascendente en la confianza pública, en la continuidad de los servicios, en la integridad institucional y en el ejercicio de los derechos fundamentales de la ciudadanía. En esta línea, el presente plan se formula dando cumplimiento al régimen normativo y principalmente con el objetivo de mejorar la cultura institucional en materia de seguridad de la información y privacidad respecto a la información, promoviendo una gestión responsable, preventiva y basada en riesgos.

Este plan define y estructura las actividades dirigidas a prevenir, detectar, gestionar y responder de forma oportuna y eficaz a los riesgos y amenazas que puedan comprometer los activos de información del Ministerio, integrando la gestión del riesgo, la mejora continua y el gobierno de la seguridad de la información, de acuerdo con los principios contenidos en el Modelo de Seguridad y Privacidad de la Información –MSPI– y la estructura de alto nivel de la norma ISO/IEC 27001:2022.



De igual manera, se encuentra articulado y alineado con respecto a los demás planes, políticas y estrategias institucionales del Ministerio, de manera especial del Modelo Integrado de Planeación y Gestión –MIPG–, del Plan Estratégico Institucional, del Plan de Acción Anual, de la Estrategia de Gobierno Digital, del Plan de Tratamiento de Riesgos, del Programa Integral de Protección de Datos Personales y de los planes relacionados con continuidad y con la gestión de tecnologías de la información, asegurando coherencia, complementariedad y un enfoque integral en la gestión de la seguridad y privacidad de la información.

Con su implementación, el Ministerio reafirma su compromiso con la protección de la información y la privacidad, asegurando que sus procesos, servicios y sistemas de información estén diseñados y operados para enfrentar los riesgos cibernéticos, cumplir con la legislación vigente y garantizar la continuidad, confiabilidad y calidad de los servicios que presta a la ciudadanía.

2. OBJETIVO

Definir y ejecutar las actividades necesarias para incrementar de manera progresiva el nivel de madurez en seguridad y privacidad de la información del Ministerio de Agricultura y Desarrollo Rural durante la vigencia 2026, en concordancia con el estándar internacional ISO/IEC 27001:2022, las estrategias de Gobierno Digital, el Modelo Integrado de Planeación y Gestión –MIPG–, los lineamientos del Modelo de Seguridad y Privacidad de la Información –MSPI–, los requerimientos institucionales y las disposiciones legales vigentes.

2.1 OBJETIVOS ESPECÍFICOS

- Establecer y divulgar las actividades para el fortalecimiento de la seguridad y privacidad de la información en la entidad.
- Incrementar el nivel de madurez del MADR frente a la gestión de la seguridad y privacidad de la información.
- Fortalecer y optimizar la gestión de seguridad y privacidad de la información en la entidad.
- Gestionar los riesgos de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad del negocio que puedan afectar la integridad, confidencialidad, disponibilidad y privacidad de la información.
- Asegurar la protección de los activos de información de la Entidad, a través de la identificación, clasificación y/o actualización de los activos de información y sus riesgos asociados
- Gestionar de manera oportuna los eventos e incidentes de seguridad de la información que pongan en riesgo la integridad, confidencialidad, disponibilidad y privacidad, reduciendo su impacto y propagación.
- Fortalecer la cultura, el conocimiento y las habilidades de los colaboradores en los temas de seguridad y privacidad de la información en el MADR..



3. ALCANCE

El Plan de Seguridad y Privacidad de la Información del Ministerio de Agricultura y Desarrollo Rural aplica a todos los procesos, dependencias, servidores públicos, contratistas y terceros que, en el ejercicio de sus funciones, tengan acceso, administren, procesen, almacenen, transmitan o dispongan de activos de información del Ministerio, independientemente del medio, formato o tecnología utilizada.

Adicionalmente el alcance del plan se extiende a la protección de los activos de información que están asociadas con los sistemas de información, infraestructuras tecnológicas, servicios digitales, plataformas en la nube, bases de datos, documentos físicos y electrónicos, así como con la información personal, información sensible, información estratégica, etc., que son de responsabilidad del Ministerio, durante todas las etapas de su ciclo de vida, etc.

El alcance no está limitado a la utilización de controles técnicos, sino que integran controles administrativos, organizacionales y también legales que permiten una gestión integral de los riesgos de seguridad y privacidad de la información, de la normativa aplicable lo que propende en la mejora de la cultura institucional de la seguridad, garantizando la confidencialidad, la integridad, la disponibilidad, la privacidad, de la información que soporta la misión y los servicios del Ministerio.

4. 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, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
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"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley Estatutaria 1581 de 2012	Reglamentada parcialmente por el Decreto Nacional 1377 de 2013, Reglamentada Parcialmente por el Decreto 1081 de 2015. Ver sentencia C-748 de 2011. Ver Decreto 255 de 2022. 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".
Artículo 2.2.2.25.3.1, del Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, 1074 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo



Agricultura

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.
Artículo 2.1.1.1.1, del Decreto Único Reglamentario del Sector Presidencia de la República, 1081 de 2015	Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Decreto 767 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
CONPES 3854 de 2016	Política Nacional de Seguridad Digital del Estado Colombiano
Decreto 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015
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 3995 de 2020	Política Nacional De Confianza y Seguridad Digital
Decreto 338 de 2022	Por el cual se adiciona el Título 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 1519 de 2020, expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones	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 500 de 2021, expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones	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
Resolución 746 de 2022, expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones	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 2277 de 2025, expedida por el Ministerio de Tecnologías de la Información y	Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia



Agricultura

las Comunicaciones	
--------------------	--



5. DESARROLLO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

FASE	ACTIVIDADES	DEPENDENCIA RESPONSABLE:	PRODUCTO / ENTREGABLE:	FECHA
PLANEACION	Definir la estrategia de seguridad y privacidad de la información, detallando actividades específicas para el 2026.	Oficina de Tecnologías de la Información y las Comunicaciones	Anexo de la estrategia de seguridad y privacidad de la información,	Enero a Febrero
	Definir plan de sensibilización en seguridad y privacidad de la información.	Oficina de Tecnologías de la Información y las Comunicaciones	Plan de sensibilización privacidad de la información.	Enero a Febrero
	Definir plan inicial de seguridad y privacidad de la información para la vigencia 2027	Oficina de Tecnologías de la Información y las Comunicaciones	Propuesta del plan seguridad y privacidad de la información 2027	Noviembre Diciembre
IMPLEMENTACIÓN	Fortalecer el programa integral de Protección de Datos personales mediante la implementación de controles de seguridad y privacidad.	Oficina de Tecnologías de la Información y las Comunicaciones	Controles implementados para el fortalecimiento del programa integral de Datos Personales de acuerdo con el alcance definido en la estrategia de seguridad y privacidad de la información.	Marzo a Noviembre
	Implementación de controles conforme con la brecha del 2025.	Oficina de Tecnologías de la Información y las Comunicaciones	Controles implementados	Marzo a Noviembre
	Realizar la gestión de incidentes de seguridad de la información al interior de la entidad.	Oficina de Tecnologías de la Información y las Comunicaciones	Gestión de incidentes realizadas	Marzo a Noviembre
	Realizar la gestión de vulnerabilidades al interior de la entidad.	Oficina de Tecnologías de la Información y las Comunicaciones	Gestión de vulnerabilidades realizadas	Marzo a Noviembre
	Actualizar los activos de información, riesgos de seguridad digital y planes de tratamiento de riesgos definidos en la entidad, alineados con las directrices de gestión de información pública de la ley 1712 del 2014.	Oficina de Tecnologías de la Información y las Comunicaciones	Activos de información, riesgos de seguridad digital, planes de tratamiento de riesgos actualizados, aprobados y publicados incluido el índice de información clasificada.	Marzo a Diciembre
	Ejecutar el plan de sensibilización en seguridad y privacidad de la información.	Oficina de Tecnologías de la Información y las Comunicaciones	Evidencias de la ejecución del plan	Marzo a Diciembre



Agricultura

SEGUIMIENTO	Realizar seguimiento al cumplimiento del plan seguridad y privacidad de la información.	Oficina de Tecnologías de la Información y las Comunicaciones	Actas o informes de seguimiento a la ejecución del plan.	Marzo a Diciembre
	Realizar seguimiento a la gestión de vulnerabilidades técnicas y a la atención de incidentes de seguridad de la información,	Oficina de Tecnologías de la Información y las Comunicaciones	Informe de seguimiento a vulnerabilidades e incidentes de seguridad de la información.	Marzo a Diciembre
MEJORA CONTINUA	Actualizar autodiagnóstico de seguridad de la información - MSPI	Oficina de Tecnologías de la Información y las Comunicaciones	Autodiagnóstico de seguridad de la información – MSPI actualizado	Mayo Noviembre
	Formular actualizar y hacer seguimiento a planes de mejoramiento derivados de los resultados de seguimiento o auditorías internas o evaluación del SGSI.	Oficina de Tecnologías de la Información y las Comunicaciones	Planes de mejoramiento definidos	Febrero a Noviembre



6. MECANISMOS DE SEGUIMIENTO

A continuación, se describen los mecanismos de seguimiento definidos para verificar el cumplimiento del Plan de Seguridad y Privacidad de la Información, así como la periodicidad con la que se realiza dicho seguimiento, en el marco de los instrumentos de planeación y los espacios de gobernanza institucional.

MECANISMO	PERIODICIDAD
Plan de Acción Institucional	Trimestral
Matrices de Riesgo	Semestral
Comité Institucional de Gestión y Desempeño	Cada vez que sesione