PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE AGRICULTURA Y DESARROLLO RURAL

2026

1. INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad de la Información del Ministerio de Agricultura y Desarrollo Rural, para la vigencia 2026, se encuentra alineado con el Plan de Seguridad y Privacidad de la Información, la Guía para la Administración de Riesgos correspondiente al Sistema de Gestión Institucional y los lineamientos del Modelo de Seguridad y Privacidad de la Información –MSPI–, incorporando las buenas prácticas de las normas internacionales ISO

Este Plan constituye un instrumento fundamental para la gestión sistemática y basada en riesgos de la seguridad de la información, toda vez que permite articular los resultados del análisis y la evaluación de riesgos con la implementación de controles adecuados y proporcionales, fortaleciendo cada uno de los procesos y procedimientos definidos en las áreas del Ministerio en el marco del Sistema de Gestión de Seguridad de la Información.

La adecuada definición e implementación del Plan de Tratamiento de Riesgos resulta esencial para garantizar la protección de los activos de información que soportan los procesos misionales, estratégicos y de apoyo del Ministerio, así como para asegurar la continuidad de los servicios y la confianza de los ciudadanos y demás partes interesadas. Un tratamiento de riesgos eficaz permite priorizar recursos, focalizar esfuerzos y establecer responsabilidades claras frente a la mitigación de las amenazas y vulnerabilidades identificadas.

De igual manera, este Plan contribuye al fortalecimiento de la cultura institucional de seguridad de la información, ya que promueve una gestión preventiva, coordinada y orientada a la mejora continua, en la que la protección de los activos de información es entendida como un elemento transversal a la gestión pública. Así, el Ministerio avanza en la consolidación de un enfoque integral de seguridad y privacidad de la información, alineado con los objetivos estratégicos institucionales y con las exigencias normativas vigentes.

2. OBJETIVO

Definir e implementar las actividades de tratamiento que permitan reducir los riesgos de seguridad de la información a niveles aceptables, de acuerdo con los resultados del análisis y evaluación de riesgos, priorizando los activos de información críticos del Ministerio de Agricultura y Desarrollo Rural.

2.1 OBJETIVOS ESPECÍFICOS

- Fortalecer la gestión institucional de los riesgos de seguridad de la información mediante la aplicación de controles técnicos, administrativos y organizacionales alineados con el estándar ISO/IEC 27001:2022, el Modelo de Seguridad y Privacidad de la Información –MSPI– y el marco normativo vigente.

- Implementar actividades técnicas que permitan gestionar los riesgos de seguridad de la información.

- Implementar actividades organizacionales que permitan gestionar los riesgos de seguridad de la información.

- Implementar actividades administrativas que permitan gestionar los riesgos de seguridad de la información.

3. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad de la Información del Ministerio de Agricultura y Desarrollo Rural aplica para todos los activos de información identificados y valorados en el marco del Sistema de Gestión de Seguridad de la Información, incluyendo información en formato físico y digital, sistemas de información, infraestructuras tecnológicas, servicios TIC, plataformas en la nube y datos personales bajo responsabilidad del Ministerio, cuyo nivel de riesgo residual sea establecido en moderado o alto.

El alcance del Plan comprende la definición, ejecución y seguimiento de las acciones de tratamiento de riesgos que involucren a los procesos misionales, estratégicos y de apoyo, conforme como está definido en la política de administración de riesgos de la entidad.

4. MARCO NORMATIVO APLICABLE

Marco Normativo	Descripción
Ley Estatutaria 1266 de2008	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 (Complilado por el Decreto 1080 de 2015)	Por el cual se reglamenta el Título V de la Ley 594 de 2000 y se dictanotras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".
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 de 2014 y se dictan otras disposiciones.
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
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
CONPES 3995 de 2020	Política Nacional De Confianza y Seguridad Digital
Decreto 338 de 2022	Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Unico 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 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 las Comunicaciones	Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia

OTRAS NORMAS Y GUIAS ALINEADAS

- **Modelo de Seguridad y Privacidad de la Información de MINTIC:** Tiene como objetivo preservar la confidencialidad, integridad y disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

- **NORMA ISO 27001:2022:** Estándar internación que tiene como objetivo sugerir lineamientos y buenas prácticas a cualquier tipo de organización o entidad para el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

- **ISO 31000:2018:** Tiene como objetivo sugerir lineamientos y buenas prácticas a cualquier tipo de organización o entidad, para incorporar estándares y procesos de alto nivel para evaluar y mitigar riesgos en todas sus operaciones.

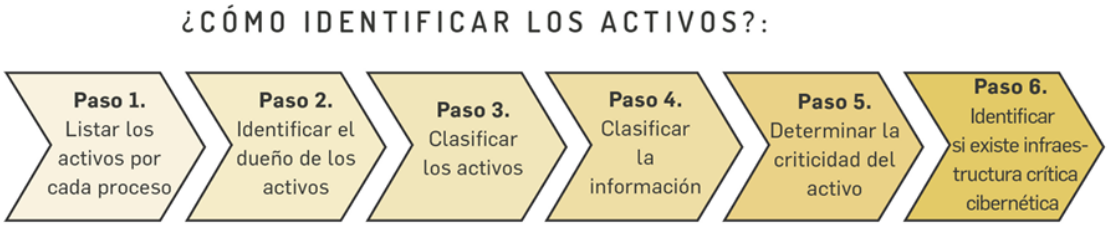
- Guía para la administración del riesgo y el diseño de controles en entidades públicas Riesgos de gestión, corrupción y seguridad digital - Versión 6 emitida por el DAFP.

- Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas

5. METODOLOGÍA DEL PLAN DE TRATAMIENTO DE RIESGOS

- **Identificación y valoración de activos de información**

Identificación de los responsables de los activos de información quienes son los responsables de realizar la identificación y categorización de estos. La identificación y valoración de activos de información se realiza conforme a lo establecido en el Modelo de Gestión de Riesgos de Seguridad Digital del Anexo 4. Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas, imagen1.



Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

- **Identificación de riesgos**

Los riesgos asociados a los activos de información institucionales se clasifican en pérdida de la confidencialidad, pérdida de la integridad o pérdida de la disponibilidad.

- **Valoración de amenazas y vulnerabilidades (causas)**

Identificación de amenazas y vulnerabilidades asociadas a los activos de información institucionales según el riesgo valorado, de acuerdo con la Norma ISO 27005 y el Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas.

- **Determinación del nivel de riesgo de seguridad de la información**

La determinación del nivel de riesgo de seguridad de la información es la combinación de la valoración de los activos de información, el nivel de amenaza y la valoración de la probabilidad de la vulnerabilidad; para tal fin se define la metodología de valoración de riesgos que permite ubicar los riesgos identificados en un mapa de calor de clasificación de riesgos según la criticidad de los activos, de esta ubicación se determina el nivel de riesgo aceptable.

- **Gestión del Riesgo**

De acuerdo con la determinación del Nivel de Riesgo de Seguridad de la Información, se establece para la gestión de riesgos, las siguientes acciones:

Aceptar el riesgo: Riesgos en nivel bajo. No se debe realizar ninguna acción o actividad por parte de los responsables de los riesgos (primera línea de defensa). Sin embargo, es importante que se realice el respectivo seguimiento y monitoreo.

Reducir el riesgo (Mitigar): Riesgos en nivel moderado, alto o extremo. Se adoptan medidas adicionales a los controles implementados para cada uno de los activos de información, con el fin de reducir la probabilidad e impacto del riesgo.

Reducir el riesgo (Transferir): Riesgos en nivel moderado, alto o extremo. Se realiza la tercerización del riesgo / transferencia del riesgo a un tercero. (ej. Seguros), con el fin de reducir la probabilidad e impacto del riesgo.

Evitar el riesgo: NO se asumen las actividades que generan el riesgo.

Ilustración 1 Acciones de plan de tratamiento de riesgos

Fuente: Tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6.

6. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN / SEGURIDAD DIGITAL

De acuerdo como se tienen identificados los activos de información se establece el siguiente plan de tratamiento de riesgos de seguridad de la información, para la vigencia 2026.

Actividad	Descripción de la actividad	Fecha	Responsable
Revisión del inventario de activos de información	Verificar que los activos de información identificados estén completos, actualizados y cuenten con responsable asignado (dueño del activo).	FEBRERO	Oficial de Seguridad de la Información
Revisión de riesgos generales asociados a los activos	Analizar los riesgos identificados para cada activo, validando su coherencia con el contexto de la entidad y los procesos misionales y de apoyo.	MARZO-ABRIL	Oficial de Seguridad de la Información
Identificación de controles de seguridad requeridos	Consolidar los controles de seguridad definidos como requeridos para cada riesgo (técnicos, administrativos y físicos), alineados con ISO 27001/MSPI.	MAYO-JUNIO	Oficial de Seguridad de la Información
Verificación de controles de seguridad implementados	Validar, mediante evidencia documental y técnica, qué controles se encuentran efectivamente implementados, parcialmente implementados o no implementados.	MAYO-JUNIO	Oficial de Seguridad de la Información
Revisión de evidencias de control	Recopilar evidencias: políticas, procedimientos, configuraciones, bitácoras, reportes, contratos,	MAYO-JUNIO	Oficial de Seguridad de la Información

Actividad	Descripción de la actividad	Fecha	Responsable
	actas o registros que soporten la implementación de controles.		
Análisis de brechas de control.	Identificar brechas entre los controles requeridos y los controles realmente implementados, determinando debilidades y riesgos residuales preliminares.	JULIO	Oficial de Seguridad de la Información
Elaboración del informe	Consolidar informe del análisis de brechas identificadas.	JULIO	Oficial de Seguridad de la Información

7. MECANISMOS DE SEGUIMIENTO

A continuación, se describen los mecanismos de seguimiento definidos para verificar el cumplimiento del Plan de Tratamiento de Riesgos de Seguridad 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.

MECANSIMO	PERIODICIDAD
Plan de Acción Institucional	Trimestral
Comité Institucional de Gestión y Desempeño	Cada vez que sesione

8. DEFINICIONES

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

(ISO/IEC 27000).

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Riesgo: 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. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información - SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).