MINISTERIO DE AGRICULTURA Y DESARROLLO RURAL
OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2024

1. INTRODUCCIÓN

El Plan de Seguridad y Privacidad de la Información del Ministerio de Agricultura y Desarrollo Rural, se encuentra alineado con i) la Política de Gobierno Digital, específicamente con la implementación del Modelo de Seguridad y Privacidad de la Información; ii) con la Política de Seguridad Digital en lo referente a la gestión de riesgos de seguridad digital; y iii) con la Norma ISO NTC/IEC ISO 27001:2013 de Seguridad de la Información.

Este Plan se implementa a través del Sistema de Gestión de Seguridad de la Información el cual hace parte del Sistema de Gestión Integrado y tiene como finalidad el fortalecimiento de las capacidades institucionales para gestionar, tratar y mitigar los riesgos a los cuales se encuentran expuestos sus activos de información, a través de la aplicación de mecanismos y controles técnicos y administrativos que propenden por la confidencialidad, integridad y disponibilidad de estos.

Con respecto a lo anterior desde la Oficina de Tecnología e Información – OTIC se implementa, mantiene y mejora el modelo de gestión de la seguridad y privacidad de la información que permita alcanzar y mantener dentro de las diferentes áreas y colaboradores una cultura y conciencia en el acceso y uso adecuado de la información en el MADR.

La finalidad del presente documento es presentar el plan de seguridad y privacidad de la información con el fin de definir las actividades a realizar para apoyar la implementación y el mejoramiento del sistema de gestión de seguridad de la información.

2. OBJETIVO Definir las actividades para incrementar el nivel de madurez de seguridad y privacidad de la Información en el Ministerio de Agricultura y Desarrollo Rural para la vigencia 2024, tomando como referencia las mejores prácticas de seguridad y privacidad como la ISO/IEC 27001 en su última versión, 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 la información del ministerio.

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 -MADR, comprende la implementación del Sistema de Gestión de Seguridad de la Información en sus fases del modelo de mejora continua (Planear, Hacer, Verificar y Actuar) aplicable a los procesos institucionales, y a todos los usuarios internos, externos, proveedores y a la ciudadanía en general, mediante la implementación de una estrategia integral de seguridad de la información que parta desde las políticas, prácticas y aborde toda la cadena de valor, en torno a los objetivos estratégicos de la Entidad, con el fin de diagnosticar, planear e implementar de manera coordinada acciones que sean pertinentes para que el Ministerio de Agricultura cuente con un escenario donde se apliquen buenas prácticas en materia de seguridad de la información, que conlleven a la seguridad de los sistemas, los procesos, las

personas que los ejecutan y los datos, bajo los únicos propósitos de reducir las vulnerabilidades a las que se encuentran expuestos los activos de información institucionales.

4. MARCO NORMATIVO

Marco Normativo	Descripción
Ley 1266 de 2008	Por la cual se dictan las disposiciones generales delhábeas 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, secrea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos.
Ley 1581 de 2012	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 deGestión Documental para todas las Entidades del Estado".
Decreto 2693 de 2012	Estrategia de Gobierno en Línea. Ministerio deTecnologías de la Información y las comunicaciones
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 ydel derecho de acceso a la Información pública nacionaly se dictan otras disposiciones
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales dela Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otrasdisposiciones.
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.
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 500 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.

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

El Sistema de Gestión de Seguridad de la Información hace parte del Sistema de Gestión Integrado del Ministerio de Agricultura, por lo tanto, las políticas, manuales, procedimientos, guías y demás resultantes de la implementación de controles de la NTC ISO/IEC 27001 27000 serán adoptados y formalizados en este último.

La gestión de Sistema de Gestión de Seguridad de la Información se realizará en la plataforma tecnológica que el Ministerio disponga para tal fin, en la cual se consolidará los resultados de la ejecución de las fases del ciclo PHVA.

5.1 FASE PREVIA - DIAGNOSTICO DEL MSPI

Esta fase permite por medio del uso de herramientas de diagnóstico, actividades dereconocimiento y valoración de controles de seguridad de la información, identificar cual esel estado actual de la Entidad en temas de seguridad y privacidad; el resultado de este de diagnóstico permitirá establecer el nivel de madurez en cuanto a seguridad y privacidad dela información, y así definir la hoja de ruta para las actividades en las siguientes fases del modelo.

5.1.1 Estado Actual

Teniendo en cuenta la calificación de FURAG, el MADR se encuentra en un puntaje de

86.6en seguridad digital, esto se ve reflejado en el esfuerzo realizado por la entidad para apoyar la implementación del SGSI, por lo que viene adelantando la actualización de las políticas y manual de políticas de seguridad y privacidad de la información, esto ha permitido avanzar en la identificación de los activos de información de la Entidad, de manera que a través del análisis de riesgo se pueda clasificary aplicar controles que permitan mejorar el nivel de riesgo de estos activos.

5.2 FASE DE PLANIFICACIÓN

Esta fase está estrechamente relacionada con el resultado dado en la fase de diagnóstico y el estado actual del MADR, esta fase permite la identificación de las piezas clave que van a definir y orientar las actividades para los propósitos de seguridad y privacidad.

5.2.1 Diagnóstico del MSPI

El nivel de implementación del MSPI permitirá al MADR establecer la estrategia a desarrollar para la vigencia 202 para implementar y mejorar la seguridad y privacidad de la información, para losprocesos (24 procesos) misionales, estratégicos y de apoyo de la Entidad y toda la infraestructura que los soporte. A corte de diciembre de 2022, el avance general en el ciclo PHVA, de acuerdo con la medición del instrumento de identificación de la línea base de seguridad, proporcionado por el Ministerio de Tecnologías de la Información y las Comunicaciones.

5.3 FASE DE IMPLEMENTACIÓN

Esta fase dará paso a que el MADR lleve a cabo la implementación de los requisitos base presentados el Modelo de Seguridad y privacidad de la información – MSPI y la norma ISO/IEC 27001:2013; de la misma forma llegar a la implementación de los controles, que por normativa o por resultado de la identificación de riesgos deban ser implementados.

Dentro de la estrategia de la Entidad se encuentra la definición de los propósitos de seguridad y privacidad de la información, y por ende se definirán e implementarán políticasy directrices que guíen las prácticas de protección de la información en cuanto a su confidencialidad, integridad y disponibilidad.

Estas actividades permiten que el MADR empiece a tener análisis y gestión sobre los siguientes temas en el marco de seguridad: gestión de activos, gestión de comunicaciones y operaciones, gestión de recursos humanos, gestión de terceros, gestión de seguridad física,

gestión de la continuidad de negocio, control de acceso lógico, cumplimiento regulatorio estrategia de seguridad en aplicaciones, estrategiade seguridad de datos y estrategia de seguridad tecnológica, entre otros.

5.3.1 Mapa de Ruta

A continuación, se listan las actividades que el MADR planea realizar para la vigencia 2024 en temas de seguridad y privacidad de la información:

Sistema de Gestión de Seguridad de la Información

- Revisión de la Política, Manual de Políticas de Seguridad y Privacidad de la Información (Marzo a Mayo), Responsable: Equipo Seguridad de la Información - OTIC
- Revisión de los controles de la norma ISO 27001:2013 (Junio a Diciembre), Responsable: Equipo Seguridad de la Información - OTIC
- Realizar seguimiento a los proveedores en cuanto al cumplimiento de las políticas de seguridad y privacidad de la información (Abril a Noviembre), Responsable: Equipo Seguridad de la Información - OTIC
- Revisión por la Dirección (Mayo a Junio), Responsable: Oficina Asesora de Planeación y Equipo Seguridad de la Información – OTIC
- Actualización de la declaración de aplicabilidad (Junio – Agosto), Responsable: Equipo Seguridad de la Información - OTIC
- Identificación y Reporte de cumplimiento de los indicadores de seguridad de la Información (Enero a Diciembre), Responsable: Equipo Seguridad de la Información – OTIC
- Definición del Plan de Concienciación en Seguridad y Privacidad (enero a junio), Responsable: Equipo Seguridad de la Información – Oficina de Tecnología y Comunicaciones – OTIC
- Ejecución del Plan de Concienciación en Seguridad y Privacidad (Febrero a Diciembre), Responsable: Equipo Seguridad de la Información – Oficina de Tecnología y Comunicaciones – OTIC y acompañan Oficina de Comunicaciones y Talento Humano.
- Entrenamientos y/o Sensibilizaciones en temas Seguridad y Privacidad de la información (Febrero a Diciembre), Responsable: Equipo Seguridad de la Información – Oficina de Tecnología y Comunicaciones – OTIC
- Análisis de resultados del Plan de Concienciación en Seguridad y Privacidad (Noviembre a Diciembre), Responsable: Equipo Seguridad de la Información – Oficina de Tecnología y Comunicaciones – OTIC.

- Realizar el análisis de impacto al negocio – BIA para los servicios críticos de la entidad (Marzo a Junio) Responsable: Equipo Seguridad de la Información – Oficina de Tecnología y Comunicaciones – OTIC.
- Definición del DRP (Mayo a Julio), Responsable: Equipo Seguridad de la Información – Oficina de Tecnología y Comunicaciones – OTIC.
- Realizar la planeación y ejecución de las pruebas definidas en el Plan de Continuidad Tecnológica (Julio a Diciembre), Responsable: Equipo Seguridad de la Información – Oficina de Tecnología y Comunicaciones – OTIC.

Activos de Información:

- Actualización de Instrumentos de gestión de la información pública (Junio Octubre), Responsables: Todos los procesos – acompañan Equipo Seguridad de la Información
- Publicación Instrumentos de gestión de la información pública (Octubre a Noviembre), Responsables: Oficina de Tecnología e Información – OTIC, apoya Oficina Asesora de Comunicaciones.
- Establecer los lineamientos y estrategias para el etiquetado de los activos de tipo información en medio físico y electrónico (Marzo a Junio), Responsables: Secretaria General (Gestión Documental), Sistema Integrado de Gestión y Equipo Seguridad de la Información.
- Implementación de las estrategias definidas para el etiquetado de los activos de tipo información en medio físico y electrónico (Junio a Diciembre), Responsables: Secretaria General (Gestión Documental), Sistema Integrado de Gestión y Equipo Seguridad de la Información – Oficina de Tecnología y Comunicaciones – OTIC.
- Atención, Gestión y documentación de los incidentes de seguridad de la información Equipo Seguridad de la Información – Oficina de Tecnología y Comunicaciones – OTIC.

Riesgos de Seguridad y Privacidad de la Información

- Identificación y Análisis de Riesgos Seguridad de la información (Febrero a Junio), Responsables: Todos los procesos - acompañamiento de Equipo Seguridad de la Información - OTIC
- Definición del Tratamiento de Riesgos Seguridad de la Información (Mayo a Julio), Responsables: Todos los procesos - acompañamiento de Equipo Seguridad de la Información - OTIC
- Seguimiento a la implementación de los planes de tratamiento (Julio a Diciembre), Responsable: Equipo de Seguridad de la Información

5.4 FASE DE GESTIÓN

Dado que la seguridad y privacidad de la Información es un proceso transversal a toda la Entidad el anterior mapa de ruta establecer las acciones necesarias para implementar, gestionar, realizar seguimiento, medición y cumplimiento con respecto al objetivo de la entidad de mejorar el nivel de madurez frente al MSPI, que permitan el cumplimiento de los objetivos estratégicos de la entidad, lo anterior se mediara a través de la definición de indicadores para el SGSI.

5.5 FASE DE MEJORAMIENTO CONTINUO

En las actividades definidas en el mapa de ruta se contemplan varias que aportarán al mejoramiento continuo del Sistema de Gestión de Seguridad de la Información en el MADR por lo que el objetivo de este plan es la incorporación de los temas de seguridad y privacidad de la información en todos los procesos de la entidad.

a. **Compromiso de la Dirección.**

El Plan de Seguridad y Privacidad de la Información del Ministerio de Agricultura y Desarrollo Rural, establece las actividades para la implementación y mejoramiento continuo del Modelo de Seguridad y Privacidad de la Información a través del SGSI, este debe ser socializado y aprobado por el Comité Institucional de Gestión y Desempeño CIGDE.

b. Objetivos Generales de Seguridad de la Información.

Los objetivos de seguridad de la información del Ministerio de Agricultura, definen cómo se aplica la Política General de Seguridad de la Información y contienen el compromiso de la dirección en la implementación y operación del SGSI, además de la disposición de recursos financieros, tecnológicos y humanos necesarios para tal fin; definen los requisitos de seguridad asociados al contexto de la Entidad, las responsabilidades del personal frente al manejo de los activos de información, el esquema de comunicación de los aspectos asociados al Sistema de Gestión de Seguridad de la Información y la articulación del SGSI con el SGI.