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

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 2024

1. INTRODUCCIÓN

El Ministerio de Agricultura y Desarrollo Rural en búsqueda de garantizar la Seguridad de la Información mediante un proceso de mejora continua, tiene el compromiso de definir, implementar y mantener una gestión de riesgos en Seguridad de la Información que establezca controles para proteger los activos de información que son parte fundamental para el cumplimiento de los objetivos de cada proceso en la Entidad.

La gestión de riesgos en seguridad de la información corresponde a un proceso ordenado, dinámico y transversal a toda la Entidad, el cual se desarrolla a través de actividades para el establecimiento del contexto, la identificación, valoración, evaluación, tratamiento y seguimiento para lograr el mejoramiento continuo en la Seguridad y Privacidad de la Información. De acuerdo con lo anterior, este documento contiene el plan para aplicar una estrategia de gestión de riesgos en seguridad de la información por parte de la Entidad, en búsqueda de identificar potenciales afectaciones sobre la confidencialidad, integridad, privacidad y disponibilidad, alineado con los estándares como la ISO/IEC 27001, ISO 27005, ISO 31000 en sus últimas versiones y la Guía para la administración del Riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública – DAFP, principalmente en lo dispuesto en su Anexo 4 - Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas del Ministerio de Tecnología de la Información y las comunicaciones.

ALCANCE

El Plan Tratamiento de Riesgos de Seguridad de la Información del Ministerio de Agricultura y Desarrollo Rural, 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 y Desarrollo Rural 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.

2. PLAN DE TRATAMIENTO DE RIESGOS.

El Plan de Tratamiento de Riesgos del Ministerio de Agricultura y Desarrollo Rural, define como se realiza la identificación, análisis, valoración y gestión de riesgos de seguridad de la información del Sistema de Gestión de Seguridad de la Información (SGSI), con el propósito de obtener resultados reproducibles y comparables, para lo cual se realiza:

- **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, Imagen 1.

Imagen 1. Pasos para la identificación y valoración de activos.
Fuente: Ministerio de Tecnologías de la Información y Comunicaciones

- **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.** 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 de Gestión de Riesgos de Seguridad Digital del Anexo 4. Lineamientos para la Gestión de Riesgos de Seguridad Digital 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 definirá la metodología de valoración de riesgos que permita 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.

2.1. Gestión del Riesgo.

De acuerdo con la determinación del Nivel de Riesgo de Seguridad de la Información, se establece para la gestión de riesgos, los siguientes cuatro métodos:

- ACEPTAR EL RIESGO.

- TRATAR EL RIESGO
- TRANSFERIR EL RIESGO
- EVITAR EL RIESGO

2.2. TRATAMIENTO DE RIESGOS.

A continuación, se presenta la metodología del Plan de Tratamiento de Riesgos enmarcados en las fases del ciclo de mejora continua PHVA.

PLANEAR	HACER	VERIFICAR	ACTUAR
Definir alcance SGSI	Ejecutar el plan de tratamiento de riesgos	Ejecutar el plan operacional	Implementar las mejoras identificadas
Definir la política de Seguridad de la Información	Documentar controles	Verificar el inventario de activos	Tomar medidas preventivas y correctivas
Levantamiento de inventario de **activos información**	Implementar políticas	Revisar revisiones de la eficacia	Aplicar lecciones aprendidas
Realizar análisis de riesgos	Implementar entrenamiento	Realizar revisiones del riesgo residual	Comunicar los resultados
Seleccionar controles a implementar	Gestión de la operación y recursos	Realizar revisión interna del SGSI	Garantizar el objetivo del SGSI
Definir **plan de tratamiento de riesgos**	Implementar las respuestas a incidentes	Realizar revisión por la dirección del SGSI	Revisar la política de seguridad, alcance del SGSI, Activos de la información y riesgo residual
Preparar la declaración de aplicabilidad		Registrar el impacto del SGSI	

Entre las acciones adelantadas en el Ministerio de Agricultura y Desarrollo Rural en el marco del Plan de Tratamiento de Riesgos de Seguridad de la Información se encuentran:

2.2.1. Políticas Técnicas de Seguridad de la Información.

Aportan en la implementación de los controles de Seguridad identificados en el Análisis de Riesgos realizado, y de acuerdo con la familia del control 5 de norma ISO 27002.

2.2.2. Procedimientos

Formalización en el Sistema de Gestión Integrado e implementación de procesos y procedimientos a través de los cuales se ejecuten las políticas definidas.

2.2.3. Sensibilización y Concientización.

Desarrollo de estrategias de sensibilización y formación en Seguridad de la Información que permiten involucrar a todos los actores que forman parte de la implementación del SGSI, a través de la creación de conciencia y entendimiento de los mismos, enmarcadas en diferentes temáticas de seguridad de la información, dando cumplimiento al control 7.2.2 de la Norma ISO 27002 “Concientización, educación y capacitación de la seguridad de la información”.

El diseño y desarrollo de la estrategia de sensibilización, tiene como objetivo aportar en el desarrollo de las actividades que giran alrededor de la formación de competencias en los colaboradores de la unidad, que les sirva de base en la toma de decisiones acertadas y bien informadas sobre los temas de seguridad de la información, sus actuaciones y responsabilidades que se generen.

2.2.4. Riesgos Institucionales.

Los riesgos instituciones comprenden los riesgos generales de seguridad de la información, en los cuales se definen a grandes rasgos los controles a implementar para reducir la probabilidad de materialización de riesgos de seguridad, el tratamiento de estos riesgos se desarrolla en la herramienta tecnológica de gestión de riesgos del SGSI.

2.3. Sistema de Métricas.

De acuerdo al Manual de Gobierno Digital, se realiza el seguimiento de la eficacia de la implementación del Modelo de Seguridad y Privacidad de la Información, adicionalmente se

adoptarán mecanismos de medición de eficacia en la implementación de controles contenidos en la declaratoria de aplicabilidad y de la efectividad de los mismos.

MAPA DE RUTA

#	Actividad	Fecha inicio	Fecha final	Responsable	Producto o resultado esperado
Riesgos de Seguridad y Privacidad de la Información					
1	*Identificación, documentación, análisis y valoración de Riesgos de seguridad y privacidad de la información*	*Marzo*	*Junio*	*Todos los procesos acompañamiento de Equipo Seguridad de la Información - OTIC*	*Matriz de Riesgos*
2	*Definición de planes de tratamiento para la mitigación de los riesgos*	*Marzo*	*Junio*	*Todos los procesos acompañamiento de Equipo Seguridad de la Información - OTIC*	*Planes de tratamiento*
3	*Gestión y seguimiento a la ejecución de los planes de tratamiento definidos*	*Julio*	*Diciembre*	*Todos los procesos acompañamiento de Equipo Seguridad de la Información - OTIC*	*Informes trimestrales de gestión del Tratamiento de Riesgos*
4	*Informe de cierre de los riesgos de seguridad y privacidad de la información*	*Diciembre*	*Diciembre*	*Equipo Seguridad de la Información - OTIC*	*Informe final riesgos de seguridad y privacidad de la información*