PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – (PTR)

Agencia de Desarrollo Rural

OFICINA DE TECNOLOGIAS DE LA INFORMACIÒN

Enero, 2025

TABLA DE CONTENIDO

LISTA DE TABLAS

INTRODUCCIÓN

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTR) tiene como propósito documentar las acciones estratégicas necesarias para mitigar, transferir, aceptar o evitar los riesgos relacionados con la seguridad de la información en la Agencia de Desarrollo Rural (ADR). Este documento se alinea con el Sistema Integrado de Gestión (SIG) como elemento articulador del Modelo Integrado de Planeación y Gestión (MIPG) con los demás sistemas, modelos y estrategias de gestión y desempeño aplicables a la entidad y las normas internacionales de gestión de riesgos, garantizando la protección de los activos de información y el cumplimiento de los objetivos estratégicos.

1. OBJETIVO

Establecer las actividades para realizar la gestión de riesgos de Seguridad y Privacidad de la Información, con el propósito de proteger y preservar la integridad, confidencialidad, disponibilidad y autenticidad de la información de la ADR

2. ALCANCE

La gestión de riesgos de seguridad y privacidad de la información y seguridad digital, aplica a todos los procesos establecidos en la ADR (Misionales, Estratégicos, Apoyo y de Evaluación).

3. MARCO NORMATIVO APLICABLE

- **ISO 27005**: proporciona un marco específico para la gestión de riesgos asociados a la seguridad de la información, alineada con los principios de la familia de normas ISO/IEC 27000.
- **ISO 22301**: Norma internacional diseñada para establecer, implementar, mantener y mejorar un Sistema de Gestión de Continuidad del Negocio (BCMS, por sus siglas en inglés).
- Resolución 500 de 2021 del MINTIC, sobre seguridad digital y privacidad.
- Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas - DAFP 2022.
- NTC-ISO 27001:2022 “Seguridad de la información, Ciberseguridad y Protección de la Privacidad”.
- Resolución 529 de 2024 - Por medio de la cual se adopta el Sistema Integrado de Gestión, se actualiza el Comité de Gestión y Desempeño de la ADR y se dictan otras disposiciones”
- 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”, donde se encuentra el presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, como uno de los requisitos a desarrollar para cumplir con esta normativa.

4. DEFINICIONES

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

MSPI: Modelo de Seguridad y Privacidad de la Información

Riesgo de seguridad de la información (Seguridad digital): 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: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Tratamiento del Riesgo: Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos. Existen 4 categorías para “tratar” los riesgos: aceptar el riesgo, reducir el riesgo, evitar el riesgo y compartir el riesgo.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

5.1. RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En el entorno digital, los riesgos de seguridad y privacidad de la información surgen como el resultado de la combinación de amenazas y vulnerabilidades que afectan directamente la estabilidad de sistemas críticos y el logro de objetivos estratégicos. Estos riesgos no solo comprometen aspectos técnicos, sino que también tienen implicaciones económicas, sociales y políticas, pudiendo debilitar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses estratégicos de una nación.

Por lo tanto, para este enfoque integral de riesgos la Agencia de Desarrollo Rural (ADR) adopta la guía GU-SIG-002 GUÍA PARA LA ADMINISTRACIÓN DEL RIESGOS, donde se define la metodología de identificación, clasificación, valoración y evaluación de los riesgos de forma general y en el apartado 5.5. Riesgos Seguridad de la Información específica la metodología para los riesgos de seguridad y privacidad de la información.

Tabla 1. Riesgos

CLASES DE RIESGO	DESCRIPCIÓN
Riesgos de seguridad digital	Posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

5.2. TRATAMIENTO DE RIESGOS VIGENCIA 2025

Para los riesgos residuales identificados en la vigencia de 2024 se establecieron planes de tratamiento de riesgo con base al posible impacto en la entidad, donde se especificación controles basados en policitas de seguridad de la información. Teniendo en cuenta que es un ejercicio continuo donde se realizan diagnósticos, análisis de vulnerabilidades e identificación de amenazas críticas, se contemplan planes de acción basados en el tratamiento de riesgos de seguridad y privacidad de la información, que abarcan actividades como las siguientes:

- Generación/Actualización de documentos con lineamientos y políticas de seguridad de la información de ser necesarios.
- Concientización de personal.
- Aprovechamiento de las herramientas o recursos con los que cuenta la Agencia de Desarrollo Rural.
- Inversión en controles tecnológicos que permitan el adecuado resguardo y protección de los activos de información.
- Apropiación de documento, roles y responsabilidades de seguridad de la información por parte del personal de la Oficina de Tecnología.

5.3. ACTIVIDADES DE TRATAMIENTO DE LOS RIESGOS DE PRIVACIDAD Y SEGURIDAD DE LA INOFORMACIÓN

La gestión de riesgos de privacidad y seguridad de la información es un proceso dinámico y continuo que asegura la identificación, análisis, valoración y tratamiento de los riesgos a lo largo de la vigencia 2025. El objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información, así como proteger la privacidad de los datos personales.

Para este propósito, se han definido las siguientes estrategias:

No.	Actividad	Responsable	Ejecución	
			1-Semestre	2-Semestre
1	Identificar, clasificar, analizar, valorar y evaluar los riesgos de seguridad y privacidad de la información	Líderes de proceso de la ADR – acompañamiento OTI – Equipo de Seguridad de la información	X	
2.	Definir los planes de tratamiento de los Riesgos de Seguridad y Privacidad de la Información	Líderes de proceso de la ADR – acompañamiento OTI – Equipo de Seguridad de la información	X	
3	Realizar seguimiento a los planes de tratamiento, ajustes y calibración	Líderes de proceso de la ADR – acompañamiento OTI – Equipo de Seguridad de la información	X	
4	Reportar a la OTI incidentes de seguridad y privacidad de la información	Líderes de proceso de la ADR	X	X
5	Ejecutar el plan de concientización en Seguridad de la información	Equipo de Seguridad de la información	X	X

Estas actividades se adaptarán conforme evolucione el entorno de amenazas y los objetivos organizacionales. Igualmente, serán monitoreadas para evaluar su efectividad y realizar ajustes oportunos.

6. MONITOREO Y SEGUIMIENTO DEL PLAN DE TRATAMIENTO DE RIESGOS

Es responsabilidad de los dueños de los procesos realizar el monitoreo de los riesgos y sus tratamientos, así como analizar los resultados trimestralmente conforme a la Política Integral de Gestión de Riesgos de la Entidad e ir reportando los resultados del monitoreo y su análisis, el cual debe enviarse a la oficina de planeación para su análisis y consolidación.

El responsable de la gestión de la seguridad de la información (Oficial de Seguridad) asesorará y apoyará a los líderes de proceso en la identificación de riesgos de seguridad de la información y en la definición de planes de tratamiento de estos, que serán asumidos e implementados por los líderes de proceso. De igual forma, el oficial de seguridad revisara la ejecución de los tratamientos referentes a riesgos de seguridad de la información y brindara retroalimentación a la Jefe de la Oficina de Tecnología de la Información y el jefe de la Oficina de Planeación para que sea informado a la alta dirección de la Agencia.

7. DOCUMENTOS ASOCIADOS

- Plan de seguridad y privacidad de la información.
- GU-SIG-002 Guía para la Administración de Riesgos.

8. CONTROL DE CAMBIOS

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
01	Enero 2023	Versión inicial del documento
02	Enero 2024	Actualización estado de riesgos de seguridad digital de la entidad
03	Enero 2025	Actualización de tratamiento e identificación de riesgos

ELABORÓ	REVISÓ	APROBÓ
Nombre: Giovanny Andres Palacios Cuartas **Cargo:** Contratista **Dependencia:** Oficina de Tecnologías de la información	**Nombre:** Fredy Ocampo Góngora **Cargo:** Jefe Oficina de Tecnología de la Información (E) Dependencia: Oficina de Tecnología de la Información **Nombre:** Claudia Paola Andrade Murillo **Cargo:** Contratista Dependencia: Oficina de Tecnologías de la Información	Comité institucional de Gestión y Desempeño