PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – PTR - 2023

AGENCIA DE DESARROLLO RURAL

Elaborado por: Hugo Alejandro Casallas Larrotta
Juan Carlos Valenzuela Buitrago
Revisado por: José Ricardo Acevedo, Jefe Oficina de Tecnológica de la Información
Aprobado por: Comité de Gestión y Desempeño Institucional

Control de Versiones

Versión	Fecha	Modificación
1.0	ENE-2023	Versión inicial del documento

TABLA DE CONTENIDO

1. OBJETIVO

Contextualizar el estado de los riesgos de seguridad y privacidad de la información de la Agencia de Desarrollo Rural y la gestión de su plan de tratamiento de riesgos y controles operaciones.

2. ALCANCE

El presente plan contempla todos los procesos de la entidad (Misionales, Estratégicos, Apoyo y de Evaluación), acorde al alcance definido en el Modelo de Seguridad y Privacidad de la Información (MSPI) establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC).

3. TÉRMINOS Y DEFINICIONES

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.

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

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

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

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

MSPI: Modelo de Seguridad y Privacidad de la Información

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

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

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.

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

4.1. ESTADO DEL PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Agencia de Desarrollo Rural (ADR), con base al establecimiento de su Modelo de Seguridad y Privacidad de la Información, gestiona los riesgos de seguridad de la Información (seguridad digital), que se puedan presentar y que pueden afectar el cumplimiento de la misión y visión a causa de la afectación de la integridad, confidencialidad o disponibilidad de sus activos de seguridad de la información.

La entidad tiene actualmente establecida una metodología propia basada en la ISO 27005, con la cual realiza la gestión de sus riesgos, y dentro de la cual se encuentra la etapa de tratamiento de riesgos. La metodología empleada por la agencia está alineada parcialmente a los lineamientos establecidos por el Departamento Administrativo de la Función Pública en la "*Guía para la administración del riesgo y el diseño de controles en entidades públicas*". Por lo que se requiere efectuar ajustes metodológicos para garantizar una completa concordancia con lo expuesto por parte de Función Pública.

La Agencia de Desarrollo Rural, realizó gestión de riesgos de seguridad de la información en el último trimestre de 2022, donde se realizó una identificación de riesgos de seguridad basado en los inventarios de activos de información de cada proceso y se plantearon los planes de tratamiento para mitigar las vulnerabilidades y amenazas identificadas para reducir su probabilidad de ocurrencia.

Con base al ejercicio efectuado se establecieron dieciséis (16) riesgos específicos para los procesos relacionados con tecnologías de la información y las comunicaciones (OPERACIÓN DE LOS SERVICIOS TECNOLÓGICOS Y ESTRATEGIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES) lo anterior, conforme a la identificación detallada de los activos y 59 riesgos para los demás procesos con respecto a los activos de información actualmente disponibles.

En esta etapa de gestión de riesgos a nivel institucional, no se observaron riesgos en nivel extremo, ni una cantidad considerable de riesgos en niveles Altos, de hecho, la gran mayoría de riesgos residuales están en zona moderada, lo que puede indicar que la entidad ha llevado a un nivel aceptable su exposición al riesgo.

4.2. RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la gestión de riesgos de seguridad de la información del 2022, se ejecutó un proceso detallado de gestión de riesgos sobre los activos específicos de los veinte (20) procesos de la entidad.

Respecto al inventario y clasificación de activos de información, se definieron los inventarios para los veinte (20) procesos, identificando un total de seiscientos noventa y seis (246) activos, los cuales posterior a su identificación y valoración, fueron analizados en las respectivas matrices de riesgo con la metodología propia que la Agencia a la fecha de este informe se viene manejando, la cual es una metodología de riesgos propia, parcialmente alineada con la emitida por Función Pública.

Con base a este análisis de riesgos de seguridad digital, enfocado a vulnerabilidades y amenazas, se identificaron las siguientes cantidades de riesgos clasificados por cada uno de los procesos de la entidad.

Zona de Riesgo	Cantidades
Extremo	0
Alto	68
Moderado	7
Bajo	0
Total	75

Riesgos Inherentes Gestión de Riesgos 2022

Zona de Riesgo	Cantidades
Extremo	0
Alto	7
Moderado	67
Bajo	1

Total	75

Riesgos Residuales Gestión de Riesgos 2022

Nota 1: Las vulnerabilidades, amenazas, o descripción detallada de los riesgos de seguridad de la información son información pública clasificada, teniendo en cuenta que pueden poner en riesgo la operación y activos de información de la entidad.

Nota 2: Los riesgos encontrados en la vigencia 2022 y que se tomarán como base para la elaboración de este plan, tendrán varias modificaciones por aspectos como alineación completa a la metodología de función pública, nuevas amenazas, nuevas vulnerabilidades y reevaluación de probabilidades e impactos.

4.3. RESULTADO DEL PLAN DE TRATAMIENTO DE RIESGOS VIGENCIA 2023

Para los riesgos residuales indicados en el punto **4.2** se establecieron planes de tratamiento de riesgo con base al posible impacto en la entidad. Sin embargo, teniendo en cuenta que se han identificado en ejercicios de diagnósticos vulnerabilidades y amenazas críticas, se contemplan unos planes de acción críticos para el tratamiento de estos nuevos riesgos, que abarcan actividades como las siguientes:

- Generación/Actualización de documentos con lineamientos y políticas de seguridad de la información.
- Verificación de alternativas de centros de datos.
- Asignación de roles y responsabilidades en el grupo TIC.
- 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.

Es de tener en cuenta que los riesgos serán redistribuidos para el final de la vigencia, teniendo en cuenta que la metodología de riesgos será alineada con la Guía para la administración del riesgo y el diseño de controles en entidades públicas v5 establecida en el 2020, por el Departamento Administrativo de la Función Pública (DAFP). La cual, es sugerida ser implementadas en las entidades públicas para la alineación e integración de riesgos de proceso, corrupción y seguridad digital, esta actualización implicará cambios en varios aspectos como los siguientes:

1. Modificación en la calificación de controles.
2. Modificación en la generación de probabilidad e impacto residuales.
3. Modificación del mapa de calor (zonas de riesgo crítico, alto, moderado y bajo).

4.4. 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 y en la definición de planes de tratamiento de estos, que serán asumidos e implementados por los líderes de proceso conforme lo indica Función Pública para su 1era línea de defensa estratégica.

De igual forma, revisara la ejecución de los tratamientos referentes a riesgos de seguridad de la información y brindara retroalimentación al coordinador del Grupo TIC y jefe de la Oficina de Planeación para que sea informado a la alta dirección de la Agencia.

5. COMUNICACIÓN

El presente documento será comunicado a las partes interesadas por medio de la página web de la Agencia de Desarrollo Rural como documento de conocimiento público de la organización, cumpliendo de esta forma con lo establecido en el decreto 612 de 2018.

6. RESPONSABLES

1. Representante Legal de la Entidad y Comité de Gestión y Desempeño Institucional: Aprobar los documentos de Alto Nivel
2. Secretario (a) General y de Gobierno: Velar por la implementación del MSPI y garantizar los recursos requeridos.
3. Responsable de Seguridad Digital / CIO / Enlace TIC: Coordinar las actividades de implementación del MSPI y apoyar en la definición de controles para mitigar los riesgos de seguridad.

7. APROBACIÓN

El presente plan ha sido sometido a consideración y conocimiento de la alta dirección, el comité de gestión y desempeño institucional con el objetivo de ser aprobado y aplicado conforme a lo que aquí se define.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Juan Carlos Valenzuela **Cargo: Contratista profesional** Nombre: Hugo Alejandro Casallas Larrotta **Cargo: Contratista profesional**	Nombre: Jose Ricardo Acevedo Solarte Cargo: Jefe Oficina de Tecnología de la Información	