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

AGENCIA DE DESARROLLO RURAL

2024

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

TABLA DE CONTENIDO

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

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.

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

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 para la vigencia 2023 tenía 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 no estaba alineada totalmente 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 realizó un rediseño de la metodología, con el fin de dar cumplimiento total la guía del DAFP y brindar una completa concordancia con lo expuesto por parte de Función Pública.

Con base a la liberación de la nueva política de riesgos en el mes de noviembre de 2023, La Agencia de Desarrollo Rural, inicio el proceso de actualización de riesgos con la nueva metodología de riesgos de seguridad de la información. Para este proceso, iniciando con el proceso de Tecnología de la información y las Comunicaciones.

Donde se realizó una identificación de riesgos de seguridad basado en los inventarios de activos de información 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 cinco (5) riesgos específicos relacionados con tecnologías de la información y las comunicaciones. lo anterior, conforme a la identificación detallada de los activos.

Teniendo en cuenta que es la primera ejecución de revisión de riesgos, aplicando la nueva tecnología. Se evidencia que los mismos se encuentran en nivel extremo y alto. Lo cual, es un comportamiento esperado, ya que previamente, no se habían establecido controles operacionales o de tratamientos a los mismos.

En este sentido se inició el establecimiento de tratamientos para los riesgos con el fin de llevarlos a niveles aceptables o tolerables, es decir nivel igual o menor a moderado.

4.2. RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la gestión de riesgos de seguridad de la información del 2023, se ejecutó el proceso con 1 de los 20 procesos que tiene la entidad, para la vigencia 2024, se realizara la gestión de riesgos de los 19 proceso adicionales con la nueva metodología planteada.

Respecto al inventario y clasificación de activos de información, para el primer proceso (Gestión de Tecnologias de la Información), se identificó un total de ciento no venta y ocho (198) activos, los cuales posterior a su identificación y valoración, fueron analizados en la matriz de riesgo con la nueva metodología de riesgos liberada en la Entidad.

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 y su respectiva redistribución una vez se ejecuten los controles en el 2024.

Tabla 1. Riesgos Inherentes Gestión de Riesgos 2023

Zona de Riesgo	Cantidades
Extremo	4
Alto	1
Moderado	0
Bajo	0
Total	5

Tabla 2 Proyección de riesgos Residuales Gestión de Riesgos 2024

Zona de Riesgo	Cantidades
Extremo	0
Alto	0
Moderado	5
Bajo	0
Total	5

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 2023 y que se tomarán como base para la elaboración de este plan, tendrán varias modificaciones teniendo en cuenta la gestión de riesgos de los 19 procesos adicionales que se realizara en la vigencia 2024.

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.
- 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 Técnología.

Es de tener en cuenta que los riesgos serán redistribuidos para el final de la vigencia, teniendo en cuenta el levantamiento de riesgos y activos de los 19 procesos de la entidad faltantes, con la nueva metodología de riesgos liberada por la entidad en noviembre de 2023, esta actualización implicará cambios en varios aspectos como los siguientes:

1. Identificación de nuevos activos de seguridad de la información.
2. Identificación de nuevos riesgos de seguridad de la Información.
3. Modificación en la calificación de controles.
4. Modificación en la generación de probabilidad e impacto residuales.

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 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.

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

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. Alta dirección: Velar por la implementación del MSPI y garantizar los recursos requeridos.
3. Responsable de Seguridad Digital (CISO)/ CIO / Enlace TIC: Coordinar las actividades de implementación del MSPI.

7. 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

1. 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: Hugo Alejandro Casallas Larrotta **Cargo:** Contratista profesional	**Nombre:** Olga Lucía Rivera Rodríguez **Cargo:** Jefe de la Oficina de Tecnología de la Información **Nombre:** Oscar Luis Felipe Pedraza Quintero **Cargo:** Contratista profesional	**Nombre:** Comité de Gestión y Desempeño Institucional: **Fecha:**