PLAN DE TRAMIENTO DE RIESGOS
Oficina de Tecnologías de la Información

Agencia de Desarrollo Rural
2026
Versión 04

ÍNDICE DE CONTENIDO

1 CONTROL DE CAMBIOS DEL PLAN INSTITUCIONAL

Tabla 1 Control de cambios plan en ejecución

CONTROL DE CAMBIOS PLAN EN EJECUCIÓN			
VERSIÓN	**FECHA**	**INSTANCIA DE APROBACIÓN**	**DESCRIPCIÓN**
01	Enero 2023		Versión Inicial del Documento
02	Enero 2024		Actualización estado de riesgos de seguridad digital de la entidad
03	Enero 2025	Se aprobó en el Marco del Comité de Gestión y Desempeño Institucional.	Actualización de tratamiento e identificación de riesgos
04	Diciembre 2025	Se aprobó en el Marco del Comité de Gestión y Desempeño Institucional.	Se realiza actualización de objetivos, se incorporan criterios para la identificación de riesgos de seguridad de la información

Tabla 2 Articulación Marco Estratégico

ARTICULACIÓN MARCO ESTRATÉGICO	
Objetivo de Desarrollo Sostenible	**ODS 16 – Paz, Justicia e Instituciones Sólidas** Fortalecer instituciones eficaces, responsables y transparentes, garantizando la gestión adecuada de los riesgos y la protección de la información institucional.
Plan Nacional de Desarrollo (vigencia)	**Plan Nacional de Desarrollo 2022–2026 “Colombia Potencia Mundial de la Vida”** Eje transversal: *Fortalecimiento institucional, gestión del riesgo, modernización del Estado y gobierno digital.*
Plan Estratégico Sectorial (vigencia)	**Plan Estratégico Sectorial del Sector Agricultura y Desarrollo Rural – Vigencia 2023–2026** Eje transversal: *Fortalecimiento institucional, gestión del riesgo y modernización administrativa para la adecuada implementación de la política de desarrollo rural.*
Plan Estratégico Institucional (vigencia)	**Plan Estratégico Institucional de la Agencia de Desarrollo Rural – Vigencia 2023–2026** Línea estratégica: *Fortalecimiento institucional, gestión integral del riesgo, control interno y mejora continua.*

Política Modelo Integrado de Planeación y Gestión	Política de Control Interno Política de Gobierno Digital Política de Seguridad Digital
Proceso Institucional	Gestión de Tecnologías de la Información

2 INTRODUCCIÓN

La Agencia de Desarrollo Rural a través del presente documento establece los lineamientos necesarios que contribuyen con la adecuada gestión de riesgos sobre los activos de información identificados y valorados al interior de la entidad permitiendo de esta manera establecer los controles correspondientes que prevengan y/o minimicen los impactos sobre la posible materialización de riesgos en los activos de información de la Agencia de Desarrollo Rural.

En consecuencia, por medio de los controles implementados, la Agencia de Desarrollo Rural puede controlar el grado de exposición de potenciales amenazas y/o vulnerabilidades sobre los diferentes activos de información con los que cuenta la entidad en cada una de las áreas y/o procesos de la entidad, facilitando de esta manera el adecuado y correcto uso de estos según su importancia para el cumplimiento de la misionalidad de la entidad. Así mismo, estable los roles y responsabilidades permitiendo de esta manera incorporar de manera adecuada los respectivos controles para la protección de los activos de información bajo responsabilidades de cada una de las áreas y/o procesos.

Finalmente, a través del presente documento establecen las actividades necesarias que se deben tener en cuenta al realizar los controles sobre los diferentes riesgos identificados en los activos de información, permitiendo que su elaboración contribuya con el propósito de mitigar posibles eventos y/o incidentes de seguridad de la información.

3 OBJETIVO DEL PLAN

Establecer los lineamientos a nivel de seguridad de la información que contribuyan con la prevención y/o mitigación de amenazas y/o vulnerabilidades que puedan ocasionar afectaciones en el normal funcionamiento de la confidencialidad, integridad y disponibilidad de los activos de información al interior de la Agencia de Desarrollo Rural.

3.1 Objetivos Específicos

- ✓ Evaluar por las diferentes áreas y/o procesos los riesgos asociados a los activos de información identificados que se encuentra bajo su responsabilidad.
- ✓ Definir los controles necesarios que contribuyan con la protección de los activos de información pertenecientes a las diferentes áreas y/o procesos de la Agencia de Desarrollo Rural.
- ✓ Avanzar en la implementación del Modelo de Seguridad y Privacidad de la Información que permita el mejoramiento del nivel de madurez de la Agencia de Desarrollo Rural.

4 MARCO NORMATIVO

La normativa descrita en el presente documento aborda el sustento jurídico en materia de seguridad para el desarrollo de las acciones del presente plan.

Tabla 3 Marco Normativo

TIPO DE NORMA	NÚMERO	AÑO	DESCRIPCIÓN - EPÍGRAFE
Ley Estatutaria	1266	2008	"Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".
Ley Estatutaria	1581	2012	"Por la cual se dictan disposiciones generales para la protección de datos personales"
Ley Ordinaria	603	2000	"Por la cual se modifica el artículo 47 de la Ley 222 de 1995": Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuérdese: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.
Ley Ordinaria	1273	2009	"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y los datos" - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".
Decreto Reglamentario	2573	2014	"Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones".
Decreto Reglamentario	612	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."
Decreto Reglamentario	338	2022	"[..] Establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones"
Decreto Reglamentario	767	2022	"Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital […]"
Decreto Único	1078	2015	"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
Resolución	500	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."
Resolución	746	2022	"Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución número 500 de 2021."
Resolución	2277	2025	"Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia"

5 DEFINICIONES

- ✓ **Activo de Información**: se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, documentos, soportes, edificios, personas...) que tenga valor para la organización.

- ✓ **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27001:2022)

- ✓ **Incidente de seguridad digital:** Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable. (Decreto 338 de 2022)

- ✓ **Información:** Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

- ✓ **Información Pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

- ✓ **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado.

- ✓ **Información Pública Reservada:** Es aquella información "que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos.

- ✓ **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27001:2022). Es un plan logístico detallado de cómo una entidad debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

- ✓ **Plan de Recuperación ante Desastres:** es un documento formal creado por una organización que contiene instrucciones detalladas con la definición de los procedimientos, estrategias, y roles y responsabilidades establecidos para recuperar y mantener el servicio de tecnología ante un evento de interrupción.

- ✓ **Recursos TIC:** Elemento o servicio físico o digital directamente relacionado con tecnologías de la información y las comunicaciones, pueden ser equipos de cómputo, cuentas de correo, servidores, servicios en la nube, cuentas corporativas entre otros.

- ✓ **Riesgo:** 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. (ISO/IEC 27001:2022).

- ✓ **Riesgo de seguridad digital:** Es la combinación de amenazas y/o vulnerabilidades que se pueden materializar en el curso de cualquier actividad en el entorno digital y que puede afectar el logro de los objetivos económicos o sociales al alterar la confidencialidad, integridad y disponibilidad.

6 ALCANCE

El presente Plan de Tratamiento de Riesgos aplica para todos los colaboradores, terceros y personas en general que trabajen y hagan uso de la información y/o recursos tecnológicos dispuestos por la Agencia de Desarrollo Rural, y por consiguiente su cumplimiento es de obligatorio y estricto cumplimiento al interior de la entidad.

7 DESARROLLO DEL PLAN

7.1 Diagnóstico /Articulación /Línea base

Conforme a lo identificado según la revisión realizada entre otras pero sin limitarse lo observado a través del Autodiagnóstico del Modelo de Seguridad y Privacidad de la Información, se evidencia que la Agencia de Desarrollo Rural no cuenta con una adecuada gestión de la seguridad de la información entre otros, pero sin limitarse a lo relacionado con la Gestión de Activos de Información y por consiguiente con la Gestión de Riesgos de Seguridad de la Información toda vez que tiene un rezago en este tipo de actividades desde el año 2022, siendo esta una brecha considerable a corregir teniendo en cuenta que para lograr establecer de manera adecuada controles sobre los activos de información estos deben ser identificados y valorados por las diferentes áreas y/o procesos de la entidad permitiendo de esta manera conocer la importancia que estos generan para el normal funcionamiento de la Agencia de Desarrollo Rural.

En virtud de lo anterior, para la subsanación de lo manifestado la Agencia de Desarrollo Rural a través del habilitador de Seguridad de la Información establece las siguientes acciones para su correspondiente aplicación:

7.2 Estrategias y Acciones

Tabla 4. Matriz de seguimiento de estrategias y acciones.

MATRIZ ESTRATEGIAS Y ACCIONES							SEGUIMIENTO	
ALINEACIÓN ESTRATÉGICA/ POLÍTICA MIPG ASOCIADA	**RESPONSABLE**	**ACTIVIDADES**	**RESULTADO**	**INDICADOR**	**FECHA DE INICIO**	**FECHA DE FINALIZACIÓN**	**AVANCE CUANTITATIVO**	**AVANCE CUALITATIVO**
Política de Gobierno Digital y Seguridad Digital	Todos los Procesos	Gestión de Activos de Información	Activos de Información por Proceso	Procesos con Activos Identificados / Total de Procesos de la Entidad	Marzo 2026	Julio 2026	Cuatrimestral	Cuatrimestral
Política de Gobierno Digital y Seguridad Digital	Todos los Procesos	Gestión de Riesgos Seguridad de la Información	Riesgos de Seguridad de la Información por Proceso	Procesos con Riesgos de Seguridad identificados / Total de Procesos de la entidad	Agosto 2026	Diciembre 2026	Cuatrimestral	Cuatrimestral
Política de Gobierno Digital y Seguridad Digital	Oficina de Tecnologías de la Información	Gestión de Vulnerabilidades Técnicas	Reporte de Vulnerabilidades Identificadas	Vulnerabilidades Cerradas / Vulnerabilidades Totales	Febrero 2026	Diciembre 2026	Cuatrimestral	Cuatrimestral
Política de Gobierno Digital y Seguridad Digital	Oficina de Tecnologías de la Información	Gestión de Incidentes de Seguridad de la Información	Reporte de Incidentes identificados	Incidentes Cerrados / Total Incidentes Reportados	Febrero 2026	Diciembre 2026	Cuatrimestral	Cuatrimestral

Tabla 5. Cronograma de actividades

CRONOGRAMA DE ACTIVIDADES													
Mes/ Actividad	**Ene**	**Febo**	**Mar**	**Abr**	**May**	**Jun**	**Jul**	**Ago**	**Sep**	**Oct**	**Nov**	**Dic**	**Observaciones**
Gestión de Activos de Información			X	X	X	X	X						
Riesgos de Seguridad de la Información								X	X	X	X	X	
Gestión de Vulnerabilidades Técnicas		X	X	X	X	X	X	X	X	X	X	X	
Gestión de Incidentes de Seguridad de la Información		X	X	X	X	X	X	X	X	X	X	X	

Toda vez que el presente Plan está articulado al Plan de Acción Institucional - PAI de la vigencia, como líder de cada plan, se realizará seguimiento constante a las actividades definidas en la matriz operativa.

En este sentido y a fin de tomar decisiones tempranas por parte de la alta dirección se presentará el estado del plan de manera semestral en sesión del Comité Institucional de Gestión y Desempeño.

Finalmente, es importante indicar que los informes de seguimiento realizados a este plan serán publicados en la sección oficial Transparencia en la página web, en el enlace: https://www.adr.gov.co/transparencia/plan-de-accion/

7.3 Responsables

Tabla 6. Roles y Responsabilidades Modelo de Seguridad y Privacidad de la Información.

LÍNEAS DE DEFENSA	RESPONSABILIDAD
Línea Estratégica ***(Alta Dirección y Comité de Coordinación del Sistema de Control Interno)***	✓ Este nivel analiza los riesgos y amenazas institucionales frente al cumplimiento de los planes estratégicos, tendrá la responsabilidad de definir el marco general para la gestión del riesgo (política de administración del riesgo) y garantiza el cumplimiento de los planes de la entidad. ✓ Definición y evaluación de la Política de Administración del Riesgo. La evaluación debe considerar su aplicación en la entidad, cambios en el entorno que puedan definir ajustes, dificultades para su desarrollo y riesgos emergentes.
1ª Línea de Defensa ***(Servidores públicos, funcionarios y colaboradores)*** ***Medidas de Control Interno: (Controles del día a día). Ejecutados por el equipo de trabajo.*** ***Controles de Gerencia Operativa: (Ejecutados por un Jefe, Coordinador y/o Líder)***	**Líder de Proceso** ✓ La gestión operacional identifica, evalúa, controla y mitiga los riesgos. ✓ La identificación de riesgos y el establecimiento de controles, así como su seguimiento, acorde con el diseño de dichos controles, evitando la materialización de los riesgos. **Equipo del Proceso** ✓ Participar activamente y representar al líder del proceso en la identificación de los riesgos asociados al proceso. ✓ Gestionar la aprobación de los riesgos por parte del líder del proceso. ✓ Socializar el mapa de riesgos del proceso a todo el equipo de trabajo. ✓ Coordinar la administración de los riesgos al interior de la dependencia. ✓ Proponer acciones de mejoramiento de los riesgos. ✓ Reportar a la Oficina de Planeación (Segunda Línea de Defensa) los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos. ✓ Informar a la Oficina de Planeación la materialización de un riesgo de gestión, corrupción o fiscal y a la Oficina de Tecnologías de la Información, si obedece a la materialización de un riesgo de seguridad de la información

2ª Línea de Defensa ***(Media y Alta Gerencia: Jefe de Planeación, Coordinadores de equipos de trabajo, Comité de contratación, Áreas Financiera, Oficina de Tecnologías de la Información, entre otros que generen información para el Aseguramiento de la operación)***	✓ Consolidan y analizan información sobre temas clave para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos. ✓ Asesorar a la 1ª línea de defensa en temas clave para el Sistema de Control Interno: i) riesgos y controles
3ª Línea de Defensa **Oficinas de Control Interno**	✓ Genera a través de su rol de asesoría una orientación técnica y emite recomendaciones frente a la administración del riesgo en coordinación con la Oficina de Planeación o quien haga sus veces. ✓ Monitorear la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo.

Fuente: Manual de Gestión Integral de Riesgos.

8 RECURSOS

Para la ejecución de las diferentes actividades mencionadas en el presente documento se utilizarán lo recursos correspondientes al Proyecto de Inversión ***Mejoramiento de la capacidad tecnológica de la Agencia De Desarrollo Rural.***

9 MECANISMOS DE SEGUIMIENTO Y EVALUACIÓN

9.1 Metodología de Seguimiento

Los seguimientos serán realizados ***cuatrimestralmente*** conforme a lo establecido en ***PR-SIG-010 Procedimiento Gestión Integral de Riesgos,*** teniendo en cuenta lo siguiente:

- ✓ **Criterios Identificación de Riesgos Seguridad de la Información**

Para lograr realizar una adecuada identificación de Riesgos de Seguridad de la Información cada una de las áreas y/o procesos de la Agencia de Desarrollo Rural deben realizar el levantamiento y/o actualización de los activos de información asociados facilitando de esta manera establecer la importancia de cada una de estos en función de su criticidad, para lo cual se pueden apoyar en lo establecido en ***MA-GTI 003 Manual de Gestión de Activos de Información de Seguridad de la Información.***

- ✓ **Identificación del Riesgo.**

Tiene como finalidad conocer las diferentes situaciones a las cuales se encuentra expuesto el activo de información permitiendo conocer las potenciales situaciones que puedan ocasionar afectaciones en la confidencialidad, integridad y disponibilidad de los activos de información de cada una de las áreas y/o procesos de la Agencia de Desarrollo Rural. Así las cosas, para realizar dicha identificación se debe seguir lo dispuesto en ***MA-SIG-003 Manual de Gestión de Riesgos Integral,*** a través del diligenciamiento de ***F-SIG-003 Matriz Integral de Riesgos,*** en donde se debe identificar las posibles afectaciones que se pueden presentar sobre los activos de información del proceso a nivel de:

Confidencialidad
Determina que la información no se encuentre disponible ni sea revelada a personal no autorizado tanto interno como externo.

Integridad
Determina la exactitud y completitud de la información permitiendo que esta sea precisa, coherente y completa desde su creación hasta su eliminación.

Disponibilidad
Determina la accesibilidad y utilización de la información por personal autorizado cuando esta así se requiera para su correspondiente y adecuado uso.

- ✓ **Análisis de Riesgo.**

Tiene como finalidad determinar la probabilidad de ocurrencia de los riesgos identificados junto con los correspondientes impactos producto de su materialización, permitiendo de esta manera lograr establecer de manera adecuada la clasificación del riesgo conforme a los impactos que puede llegar a generar al interior de la Agencia de Desarrollo Rural, de la siguiente manera:

Probabilidad: es la posibilidad de ocurrencia del riesgo.
Impacto: son las consecuencias que puede ocasionar la materialización del riesgo.

Así las cosas, para realizar el análisis del riesgo se deben considerar los siguientes dos (2) aspectos: Clasificación del riesgo y evaluación del riesgo.

- ✓ **Clasificación del Riesgo:**

Se determina a través de la probabilidad de ocurrencia y el impacto que significaría su materialización, teniendo en cuenta los criterios de probabilidad e impacto; donde la probabilidad debe ser medida a partir de las siguientes especificaciones:

Imagen 1. Criterios para Definición de Probabilidad.

SELECCIONE LA FRECUENCIA GENERADA DE ACUERDO A LA ESCALA MÁS IDONEA PARA EL CASO	FRECUENCIA	
	Calificación probabilidad de ocurrencia	1. Frecuencia de ejecución de la actividad generadora (DAFP)
	Descriptores de criterios para determinar el valor de la probabilidad:	1. Frecuencia de ejecución de la actividad generadora (DAFP) 2. Valor de Probabilidad asociada 3. Por Frecuencia para actividades continuas 4. Frecuencia por consolidación 5. Frecuencia en función de la exposición 6. Nivel de Oportunismo 7. Por percepción - Descriptiva
	1. MUY BAJA	La actividad que conlleva al riesgo se ejecuta como máximo 2 veces por año
	2. BAJA	La actividad que conlleva al riesgo se ejecuta entre 3-24 veces por año
	3. MODERADA	La actividad que conlleva al riesgo se ejecuta 24 a 500 veces por año
	4. ALTA	La actividad que conlleva al riesgo se ejecuta 500 a 5000 veces por año
	5. MUY ALTA	La actividad que conlleva al riesgo se ejecuta mas de 5000 veces por año

Fuente: Matriz Integral de Riesgo.

Imagen 2. Criterios para Definición de Impacto

SELECCIONE EL NIVEL DE IMPACTO GENERADO DE ACUERDO A LA ESCALA MÁS IDONEA PARA EL CASO	IMPACTO	
	Calificación probabilidad de ocurrencia	I. Afectación en la Seguridad de la Información
	Descriptores de criterios para determinar el valor de la probabilidad:	Escala para calificar el impacto de los riesgos de seguridad de la información en función de la "Criticidad del activo de información", la cual se califica de manera consolidada en la valoración de la importancia en la confidencialidad, integridad y disponibilidad del activo o grupo de activos de información
	1. MUY BAJA	Activo/ grupos de activos de criticidad baja igual a 3
	2. BAJA	Activo/ grupos de activos de información con criticidad baja igual a 4
	3. MODERADA	Activo/ grupos de activos de criticidad media, con valores de 5 y 6
	4. ALTA	Activo/ grupo de activos de criticidad alta, con valores de 7 y 8
	5. MUY ALTA	Activo/ grupos de activos de alta criticidad, con calificación = 9

Fuente: Matriz Integral de Riesgo.

- ✓ **Evaluación del Riesgo:**

Permite comparar los resultados de la calificación del riesgo, con los criterios definidos para establecer el grado de exposición en el que se encuentra la entidad; de esta manera la entidad puede determinar y distinguir entre los riesgos aceptable, tolerable, moderados, importantes y/o inaceptables y fijar las prioridades de las acciones necesarias para su tratamiento.

- ✓ **Valoración del Riesgo:**

Tiene como finalidad la consolidación de la probabilidad con el impacto, permitiendo de esta manera a cada una de las áreas y/o procesos definir las diferentes prioridades que faciliten la implantación de controles adecuados que contribuyan con la reducción de posibles materializaciones de riegos de seguridad de la Información que afecten el normal funcionamiento de la Agencia de Desarrollo Rural.

- ✓ **Monitoreo y Revisión:**

Tiene como finalidad evaluar el cumplimiento de la ejecución de controles incorporados sobre los activos de información para su adecuada protección, los cuales serán realizados ***cuatrimestralmente*** conforme a lo establecido en ***PR-SIG-010 Procedimiento Gestión Integral de Riesgos.***

- ✓ **Tratamiento de Riesgos:**

Tiene como finalidad de decidir las acciones que se toman sobre un determinado riesgo, entre los cuales se encuentran los siguientes:

Aceptar el riesgo: Si el nivel de riesgo cumple con los criterios de aceptación de riesgo, por lo que no se requiere el desarrollo de medidas de intervención adicionales a los controles existentes. La aceptación se da siempre y cuando los controles existentes se mantengan con la misma rigurosidad como fueron identificados y valorados.

Evitar el riesgo: Cuando los escenarios de riesgo identificados se consideran extremos, se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o conjunto de actividades. Para evitar el riesgo es necesario considerar la normatividad vigente y las competencias institucionales, puesto que en caso de que exista la obligatoriedad de llevar a cabo esta actividad, la opción de evitar el riesgo no se podría tomar.

Reducir el riesgo: Después de hacer un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante transferencia o mitigación de este:

Transferir el riesgo: La opción de tomar esta medida de tratamiento se podría considerar cuando existe otro proceso u entidad dispuesta a compartir una parte o la totalidad de la(s) actividad(es) que conllevan el riesgo.

Mitigar el riesgo: El nivel de riesgo debería ser administrado mediante el desarrollo de un plan de acción. Es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos

9.2 Indicadores de Seguimiento

Tabla 7. Indicadores de Seguimiento

INDICADORES DE SEGUIMIENTO					
OBJETIVO / ACCIÓN	**INDICADOR**	**FÓRMULA**	**META**	**PERIODICIDAD DE SEGUIMIENTO**	**FUENTE DE INFORMACIÓN / RESPONSABLE**
Gestión de Activos de Información	Procesos con Activos Identificados / Total de Procesos de la Entidad	Procesos con Activos Identificados / Total de Procesos de la Entidad * 100	100%	Cada 4 Meses	Matriz de Activos de Información por Procesos / Todos los Procesos
Gestión de Riesgos Seguridad de la Información	Procesos con Riesgos de Seguridad identificados / Total de Procesos de la entidad	Procesos con Riesgos de Seguridad identificados / Total de Procesos de la entidad * 100	100%	Cada 4 Meses	Matriz de Riesgos Seguridad de la Información por Procesos / Todos los Procesos
Gestión de Vulnerabilidades Técnicas	Vulnerabilidades Cerradas / Vulnerabilidades Totales	Vulnerabilidades Cerradas / Vulnerabilidades Totales * 100	75%	Cada 4 Meses	Reporte del Estado Actual de las Vulnerabilidades identificadas / Oficina de tecnologías de la Información
Gestión de Incidentes de Seguridad de la Información	Incidentes Cerrados / Total Incidentes Reportados	Incidentes Cerrados / Total Incidentes Reportados * 100	100%	Cada 6 Meses	Reporte del estado Actual de los Incidentes de Seguridad Materializados / Oficina de Tecnologías de la Información

10 RESULTADOS ESPERADOS

Con las diferentes actividades mencionadas anteriormente desde el habilitador de seguridad de la información tienen como finalidad conocer todos los elementos necesarios que son necesarios para el normal desarrollo de la misionalidad institucional con el objetivo de lograr establecer los posibles riesgos a los cuales se encuentra expuestos permitiendo de esta manera la incorporación de los controles necesarios para su adecuada protección minimizando potencialmente la probabilidad de ocurrencia de estos o en su defecto reduciendo los impactos que estos pueden llegar a ocasionar en el normal funcionamiento de la Agencia de Desarrollo Rural.

11 GESTIÓN DE RIESGOS

Tabla 8. Gestión de Riesgos

GESTIÓN DE RIESGOS				
RIESGO IDENTIFICADO	**IMPACTO**	**PROBABILIDAD**	**MEDIDAS DE TRATAMIENTO**	**RESPONSABLE**
Posibilidad de variaciones en el plan de trabajo/cronograma por incumplimiento de las actividades en los tiempos establecidos	Alto	Alto	Seguimiento continuo del avance de las actividades con los enlaces designados	Oficina de Tecnologías de la Información (Oficial de Seguridad de la Información)
Posibilidad de Cambios en normatividad relacionada con Gobierno Digital y Seguridad Digital.	Alto	Moderado	Verificar de manera continua los lineamientos emitidos por el Gobierno Nacional en Materia de Seguridad	Oficina de Tecnologías de la Información (Oficial de Seguridad de la Información y Grupo Jurídico de Oficina)
Posibilidad de desinterés o poco interés de los directivo**s**, y/o responsables de áreas y/o procesos	Alto	Alto	Compromiso por parte de la Alta Dirección para la Ejecución de las Actividades en los tiempos establecidos	Oficina de Tecnologías de la Información (Jefe de Tecnologías de la Información y Oficial de Seguridad de la Información)

12 ANEXOS

EL Plan no contiene anexos.