




	DOCUMENTO ESTRATÉGICO	VERSIÓN 9
	Política de Administración del Riesgo	DE-DEI-05 FECHA EDICIÓN 29-06-2018

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO


ELABORÓ	APROBÓ
 HERACLIO BEJARANO CRUZ Coordinador Grupo Administración del SIG FECHA: 29-06-2018	 ASTRID DEL CASTILLO SABOGA Secretaria General (E) FECHA: 29-06-2018

Handwritten mark

	DOCUMENTO ESTRATÉGICO	VERSIÓN 9
	Política de Administración del Riesgo	DE-DEI-05
		FECHA EDICIÓN 29-06-2018

CONTENIDO

1.	Objetivo.....	3
2.	Objetivos Específicos	3
3.	Alcance	3
4.	Lineamientos de la Política de Administración del Riesgo	3
5.	Historial de cambios	10

	DOCUMENTO ESTRATÉGICO	VERSIÓN 9
	Política de Administración del Riesgo	DE-DEI-05
		FECHA EDICIÓN 29-06-2018

1. OBJETIVO

La Política de Administración del Riesgo del Ministerio de Agricultura y Desarrollo Rural, tiene como propósito involucrar la gestión del riesgo como parte integral en todos los procesos de la Entidad y establecer las acciones que conduzcan a disminuir la vulnerabilidad de los mismos frente a situaciones que puedan interferir en el cumplimiento de sus funciones y objetivos institucionales.

2. OBJETIVOS ESPECÍFICOS

1. Establecer el contexto externo, interno y de los procesos de la entidad como marco de referencia para la identificación de riesgos.
2. Identificar y valorar los riesgos estratégicos, de imagen, operativos, financieros, de cumplimiento, de tecnología, de seguridad de la información y de corrupción de la entidad.
3. Establecer actividades de control de manera conjunta con los líderes de los procesos, de acuerdo al direccionamiento estratégico de la Entidad.
4. Elaborar, implementar, monitorear y revisar el mapa de riesgos institucional.
5. Promover la comunicación y consulta con las partes involucradas de la entidad durante todas las etapas del proceso para la gestión del riesgo.
6. Reducir la vulnerabilidad y fortalecer la prevención y mitigación de los efectos de los riesgos.
7. Proteger los recursos del Ministerio, resguardándolos contra la materialización de los riesgos.

3. ALCANCE

La Política de Administración del Riesgo aplica a todos los procesos del Sistema Integrado de Gestión del Ministerio de Agricultura y Desarrollo Rural y a todos los proyectos liderados por esta entidad.

4. LINEAMIENTOS DE LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO


Para el tratamiento de los riesgos, además de la aplicación del procedimiento “Para la gestión del riesgo (PR-SIG-05)”, se deben tener en cuenta los siguientes lineamientos:

a. Niveles de aceptación del riesgo:

Las directrices establecidas con relación a la aceptación de los riesgos son:

- Se toma como metodología para la evaluación y valoración de los riesgos, los criterios establecidos en las guías “para la administración del riesgo” y “para la gestión del riesgo de corrupción”, respectivamente.
- Los criterios tomados para la valoración de los riesgos son basados en la probabilidad y el impacto, los cuales se califican de 1 a 5 y se determina la zona en que queda valorada la exposición de la entidad con respecto al riesgo. Las evaluaciones son realizadas de acuerdo a las siguientes tablas:

PROBABILIDAD	IMPACTO				
	(1) Insignificante	(2) Menor	(3) Moderado	(4) Mayor	(5) Catastrófico
(1) Raro	B	B	M	A	A
(2) Improbable	B	B	M	A	E
(3) Posible	B	M	A	E	E

	DOCUMENTO ESTRATÉGICO	VERSIÓN 9
	Política de Administración del Riesgo	DE-DEI-05
		FECHA EDICIÓN 29-06-2018

PROBABILIDAD	IMPACTO				
	(1) Insignificante	(2) Menor	(3) Moderado	(4) Mayor	(5) Catastrófico
(4) Probable	M	A	A	E	E
(5) Casi seguro	A	A	E	E	E
B: Zona de riesgo baja					
M: Zona de riesgo moderada					
A: Zona de riesgo Alta					
E: Zona de riesgo extrema					

Tabla 1. Matriz de evaluación y calificación de riesgos institucionales

Para los riesgos de corrupción se evalúan con los siguientes criterios:


PROBABILIDAD	IMPACTO		
	(3) Moderado	(4) Mayor	(5) Catastrófico
(1) Raro	B	B	M
(2) Improbable	B	M	A
(3) Posible	M	A	E
(4) Probable	M	A	E
(5) Casi seguro	M	A	E
B: Zona de riesgo baja			
M: Zona de riesgo moderada			
A: Zona de riesgo Alta			
E: Zona de riesgo extrema			

Tabla 2. Matriz de evaluación y calificación para los riesgos de corrupción

- Al momento que se aplique la valoración cuantitativa inherente para los riesgos de corrupción, la probabilidad se califica seleccionando opción 1 (raro) al 5 (Casi Seguro). El impacto se puede calificar como moderado (3), mayor (4) o catastrófico (5).
- Cuando el riesgo residual sea evaluado como catastrófico, los responsables de los procesos deben establecer planes de contingencia que permitan continuar con el desarrollo de las actividades y el logro de los objetivos propuestos. Para los riesgos de corrupción siempre se deben establecer planes de contingencia, independiente de la zona donde se calificado el riesgo residual.
- Una vez evaluado los controles y establecidas las zonas en la cuales quedo calificado el riesgo residual, se puede tomar una de las opciones de manejo del riesgo de acuerdo al siguiente criterio:

ZONA EN LA CUAL QUEDO CALIFICADO EL RIESGO RESIDUAL	OPCIÓN DE MANEJO	OBSERVACIONES
Riesgo Baja, Moderado o Alta	Asumir	No hay necesidad de tomar otras medidas de control diferentes a las que se establecieron en el mapa de riesgo.
Extrema	Evitar, disminuir o compartir o transferir	Se debe establecer el plan de contingencia, en caso de materializarse el riesgo.

Tabla 3. Opciones de manejo de riesgos

	DOCUMENTO ESTRATÉGICO	VERSIÓN 9
	Política de Administración del Riesgo	DE-DEI-05
		FECHA EDICIÓN 29-06-2018

b. Criterios para calificación de los impactos:

El impacto hace referencia a la magnitud de los efectos que puede causar un riesgo cuando se materializa. A continuación se relacionan las directrices establecidas en la entidad para calificar los impactos:


- Se aplica una valoración cuantitativa de 1 a 5, de acuerdo a la siguiente tabla:

Impacto	Descripción
1 Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
2 Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
3 Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
4 Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad.
5 Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

Tabla 4. Calificación de impacto

- Para los riesgos de corrupción el impacto se puede calificar como moderado (3), mayor (4) o catastrófico (5).
- Cuando se trate los riesgos de corrupción y no se tenga claridad para seleccionar la calificación más adecuada, se puede hacer uso del siguiente cuestionario:

Nº Pregunta	Respuesta	
	SI	NO
Si el riesgo de corrupción se materializa podría...		
1 ¿Afectar al grupo de funcionarios del proceso?		
2 ¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3 ¿Afectar el cumplimiento de misión de la Entidad?		
4 ¿Afectar el cumplimiento de la misión del sector al que pertenece la Entidad?		
5 ¿Generar pérdida de confianza de la Entidad, afectando su reputación?		
6 ¿Generar pérdida de recursos económicos?		
7 ¿Afectar la generación de los productos o la prestación de servicios?		
8 ¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?		


	DOCUMENTO ESTRATÉGICO	VERSIÓN 9
	Política de Administración del Riesgo	DE-DEI-05
		FECHA EDICIÓN 29-06-2018

Nº Pregunta	Respuesta	
	SI	NO
9 ¿Generar pérdida de información de la Entidad?		
10 ¿Generar intervención de los órganos de control, de la Fiscalía, u otro ente?		
11 ¿Dar lugar a procesos sancionatorios?		
12 ¿Dar lugar a procesos disciplinarios?		
13 ¿Dar lugar a procesos fiscales?		
14 ¿Dar lugar a procesos penales?		
15 ¿Generar pérdida de credibilidad del sector?		
16 ¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17 ¿Afectar la imagen regional?		
18 ¿Afectar la imagen nacional?		
<p>Criterio: si del total de las preguntas...</p> <p>a) Responde afirmativamente de UNO a CINCO pregunta(s) genera un impacto Moderado.</p> <p>b) Responde afirmativamente de SEIS a ONCE preguntas genera un impacto Mayor.</p> <p>c) Responde afirmativamente de DOCE a DIECIOCHO preguntas genera un impacto Catastrófico.</p>		

Tabla 5. Cuestionario aplicable para establecer el impacto de los riesgos de corrupción


- Para los riesgos de “seguridad de la información” se puede recurrir a seleccionar el impacto de acuerdo a los criterios cualitativos o cuantitativos, que se muestran a continuación:

Impacto	Criterio Cuantitativo	Criterio Cualitativo
Catastrófico	<ul style="list-style-type: none"> ✓ Impacto que afecte la ejecución presupuestal en un valor $\geq 50\%$ ✓ Pérdida de cobertura en la prestación de los servicios de la entidad $\geq 50\%$. ✓ Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor $\geq 50\%$ ✓ Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor $\geq 50\%$ del presupuesto general de la entidad. 	<ul style="list-style-type: none"> ✓ Interrupción de las operaciones de la Entidad por más de cinco (5) días. ✓ Intervención por parte de un ente de control u otro ente regulador. ✓ Pérdida de Información crítica para la entidad que no se puede recuperar. ✓ Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. ✓ Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.

	DOCUMENTO ESTRATÉGICO	VERSIÓN 9
	Política de Administración del Riesgo	DE-DEI-05
		FECHA EDICIÓN 29-06-2018

Impacto	Criterio Cuantitativo	Criterio Cualitativo
Mayor	<ul style="list-style-type: none"> ✓ Impacto que afecte la ejecución presupuestal en un valor $\geq 20\%$ y menor al 49% ✓ Pérdida de cobertura en la prestación de los servicios de la entidad $\geq 20\%$ y menor al 49% ✓ Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor $\geq 20\%$ y menor al 49% ✓ Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor $\geq 20\%$ y menor al 49% del presupuesto general de la entidad. 	<ul style="list-style-type: none"> ✓ Interrupción de las operaciones de la Entidad por más de dos (2) días. ✓ Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. ✓ Sanción por parte ente de control u otro ente regulador. Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. ✓ Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos
Moderado	<ul style="list-style-type: none"> ✓ Impacto que afecte la ejecución presupuestal en un valor $\geq 5\%$ y menor al 20% ✓ Pérdida de cobertura en la prestación de los servicios de la entidad $\geq 10\%$ y menor al 19% ✓ Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor $\geq 5\%$ y menor al 19% ✓ Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor $\geq 5\%$ y menor al 19% del presupuesto general de la entidad. 	<ul style="list-style-type: none"> ✓ Interrupción de las operaciones de la Entidad por un (1) día. ✓ Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. ✓ Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. ✓ Reproceso de actividades y aumento de carga operativa. ✓ Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. ✓ Investigaciones penales, fiscales o disciplinarias.
Menor	<ul style="list-style-type: none"> ✓ Impacto que afecte la ejecución presupuestal en un valor $\leq 1\%$ y menor al 4% ✓ Pérdida de cobertura en la prestación de los servicios de la entidad $\leq 5\%$. ✓ Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor $\leq 1\%$ ✓ Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor $\leq 1\%$ del presupuesto general de la entidad. 	<ul style="list-style-type: none"> ✓ Interrupción de las operaciones de la Entidad por algunas horas. Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. ✓ Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
Insignificante	<ul style="list-style-type: none"> ✓ Impacto que afecte la ejecución presupuestal en un valor $\leq 0,5\%$ ✓ Pérdida de cobertura en la prestación de los servicios de la entidad $\leq 1\%$. ✓ Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor $\leq 0,5\%$ ✓ Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor $\leq 0,5\%$ del presupuesto general de la entidad. 	<ul style="list-style-type: none"> ✓ No hay interrupción de las operaciones de la entidad. ✓ No se generan sanciones económicas o administrativas. ✓ No se afecta la imagen institucional de forma significativa.

Tabla 6. Criterios para evaluar el impacto en los riesgos de seguridad de la información


	DOCUMENTO ESTRATÉGICO	VERSIÓN 9
	Política de Administración del Riesgo	DE-DEI-05
		FECHA EDICIÓN 29-06-2018

- Siempre que el impacto del riesgo residual sea calificado como catastrófico o igual a 5, el responsable del proceso debe diseñar planes de contingencia, para proteger su actividad en caso de ocurrencia o materialización.

c. Tratamiento del riesgo:

- Con base en la valoración de los riesgos, los responsables de los procesos, deben tomar decisiones adecuadas para el manejo de los riesgos, teniendo en cuenta las siguientes opciones:
 - **Evitar el riesgo**, tomar las medidas encaminadas a prevenir su materialización.
 - **Reducir el riesgo**, implica tomar medidas encaminadas a disminuir tanto la probabilidad como el impacto.
 - **Compartir o transferir el riesgo**, reduce su efecto a través del traspaso de las pérdidas (información, recursos u otros) a otras organizaciones o la distribución de una porción del riesgo con otra entidad.
 - **Asumir el riesgo**, luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el responsable del proceso acepta la pérdida residual probable. Esta opción implica equilibrar costos y esfuerzos en su implementación, considerando la viabilidad jurídica, técnica, institucional, económica y costo- beneficio.
- Cuando se toma las opciones “evitar el riesgo” o “reducir el riesgo” el responsable del proceso debe establecer acciones que demuestren que el riesgo se evitó o se redujo. Estas acciones las puede documentar en el Plan de Contingencia.
- Para los riesgos de corrupción se toman las opciones “evitar el riesgo” o “reducir el riesgo”.
- Los riesgos identificados en las matrices para los procesos actuales, son los mismos que se establecen en los requerimientos de la norma ISO 9001:2015.
- Los controles para el tratamiento de los riesgos “Seguridad de la información” son seleccionados por la Oficina de Tecnologías de la Información y las Comunicaciones, de acuerdo a los parámetros definidos en la Norma Técnica NTC ISO 27001, especialmente aquellos controles recomendados en el Anexo A de la misma, así mismo los responsables de los procesos deben implementarlos.
- Los procesos que hayan identificado riesgos que no posean controles, deben diseñar controles para evitar la materialización del riesgo o establecer acciones preventivas para eliminar la causa del posible riesgo.
- Los procesos que hayan identificado riesgos que no posean controles, deben diseñar controles para evitar la materialización del riesgo o establecer acciones preventivas para eliminar la causa del posible riesgo.
- Cuando se diseñen nuevos controles, los responsables de los procesos deben comunicarlo al Proceso Administración del Sistema Integrado de Gestión, a efectos de actualización de los mapas de riesgos.


d. Periodicidad para el seguimiento de acuerdo al nivel de riesgo residual:

	DOCUMENTO ESTRATÉGICO	VERSIÓN 9
	Política de Administración del Riesgo	DE-DEI-05
		FECHA EDICIÓN 29-06-2018

- El Grupo Administración del SIG es responsable de apoyar a las dependencias en la identificación de los riesgos y mantener actualizado los procedimientos respectivos. Los mapas de riesgos establecidos, se revisarán al menos una vez al año y se ajustarán si es necesario para adaptarlos a los cambios, situaciones o circunstancias por las que pueda atravesar la Entidad.
- La Oficina de Tecnologías de la Información y las Comunicaciones, es responsable de orientar a las dependencias del Ministerio en la identificación de los riesgos “tecnológicos” y de “seguridad de la información” e identificarlos en coordinación con el Grupo Administración del SIG. Los mapas de riesgos establecidos, se revisarán al menos una vez al año y se ajustarán si es necesario para adaptarlos a los cambios, situaciones o circunstancias por las que pueda atravesar la Entidad.
- La Oficina de Control Interno es responsable de realizar el seguimiento y evaluación a los riesgos identificados en los mapas de riesgos, de acuerdo con la planeación establecida para las auditorías a realizar durante la vigencia.
- La Política de Administración del Riesgo se revisará cada vez que sea requerido por parte del Representante de la Alta Dirección teniendo en cuenta los comentarios y lineamientos del Comité Institucional de Gestión y Desempeño.

e. Niveles de responsabilidad sobre el seguimiento y evaluación de los riesgos:


- Los responsables de los procesos, deben identificar los riesgos que puedan afectar el desarrollo de las actividades de los procesos o el logro de los objetivos propuestos. Cuando en una actividad no se considere la identificación de riesgos, estos no se registran en la matriz de riesgos, pero es responsabilidad del responsable del proceso mantener la revisión permanente para identificar si se identifica algún riesgo y formalizarlo.
- Los responsables de los procesos misionales deben identificar los riesgos que puedan afectar cada uno de los instrumentos de política formulados y determinar los controles que permitan disminuir su impacto y/o la probabilidad de ocurrencia.
- Los responsables de los procesos deben adelantar las acciones correctivas, preventivas o mejora ante las situaciones detectadas por la Oficina de Control Interno, cuando así se requiera, aplicando el procedimiento “Acciones Preventivas, Correctivas y de Mejora PR-SIG-06”
- Para los riesgos “tecnológicos” y de “seguridad de la información” los planes de tratamiento para implementación de los controles establecidos, son responsabilidad de los responsables de los procesos. En los casos que se requiera pueden solicitar la orientación a la Oficina de Tecnologías de la Información y las Comunicaciones.
- Los responsables de los procesos deben determinar la pertinencia de sus controles definidos para los riesgos identificados. Esta pertinencia la deben definir teniendo en cuenta la eficacia, eficiencia y efectividad del control para evitar que se materialice el riesgo. En caso de considerarlo que no es pertinente se debe ajustar o modificar el mapa de riesgos.
- Los responsables de los procesos deben garantizar los recursos (físicos, financieros y talento humano) que sean requeridos para mantener los controles que se establezcan, para evitar que se materialicen los riesgos.

	DOCUMENTO ESTRATÉGICO	VERSIÓN 9
	Política de Administración del Riesgo	DE-DEI-05
		FECHA EDICIÓN 29-06-2018

- Los responsables de los procesos deben mantener las evidencias de la aplicación de los controles definidos para los riesgos identificados.
- Para los riesgos “seguridad de la información” los responsables de los procesos deben adelantar las actividades necesarias para que los controles identificados sean implementados en el proceso, de acuerdo a las orientaciones dadas por la Oficina de Tecnologías de la Información y las Comunicaciones.
- Cuando se materialice un riesgo el responsable del proceso debe implementar las acciones correctivas respectivas y formalizarlas ante el Grupo Administración del SIG, aplicando el procedimiento “Acciones Preventivas, Correctivas y de Mejora PR-SIG-06”.
- Las acciones preventivas que se identifiquen con relación a los riesgos deben estar orientadas en lo posible a que el riesgo residual se reduzca y se ubique en una zona de menor impacto. La formalización de dichas acciones se realizará ante el Grupo Administración del SIG, aplicando el procedimiento “Acciones Preventivas, Correctivas y de Mejora PR-SIG-06”.
- El Grupo Administración del SIG publicará en la página WEB de la entidad los riesgos institucionales y los de corrupción, por separado, en forma consolidada, para conocimiento de la ciudadanía.
- El Grupo Administración del SIG publicará en la Intranet CAMPONET, los mapas de riesgos elaborados y aprobados para cada uno de los procesos, para consulta de los funcionarios y contratistas de la entidad.

5. HISTORIAL DE CAMBIOS

Fecha	Versión	Descripción
16-06-2009	2	Se incluyeron los numerales 3.1, 3.4, 3.7, y 3.9. Se modificó el numeral 3.6 cambiando la formulación de acciones preventivas por planes de contingencia.
30-11-2009	3	Se incluyó el numeral 3.11 y el Historial de Cambios.
10-08-2010	4	Se incluyó el numeral 3.2 y se eliminó el 3.6.
27-05-2014	5	Se incluyó el numeral 3.5, 3.9, 3.16, se modificó los numerales 3.6, 3.12, 3.15
08-04-2015	6	Se modificó el numeral 3, para ajustarlo a los lineamientos contemplados en la guía para la administración del riesgo, del DAFP (versión septiembre de 2011).

	DOCUMENTO ESTRATÉGICO		VERSIÓN 9
	Política de Administración del Riesgo		DE-DEI-05
			FECHA EDICIÓN 29-06-2018

24-05-2016	7	Se revisó el documento en su contenido general, se incorporó dentro de los lineamientos de la política, lo referente a los riesgos de “Seguridad de la información” y se actualizó los lineamientos relacionados con los riesgos de corrupción, de acuerdo a lo establecido en la “Guía para la Gestión del Riesgo de Corrupción” (versión 2015).
04-04-2016	8	Se adicionó en el numeral 3.a. lo referente a la responsabilidad de los planes de tratamiento de riesgos por parte de los dueños de los procesos para los riesgos “tecnológicos” y de “seguridad de la información” y se cambió el “Comité de Coordinación del SIG” por “Comité Institucional de Desarrollo Administrativo”.
29-06-2018	9	Se ajustó la estructura general de acuerdo a la guía “para la administración del riesgo”, del Departamento Administrativo de la Función-DAFP (versión 3, diciembre de 2014).

Proyecto: Heraclio Bejarano Cruz
 Coordinador Grupo Administración del SIG