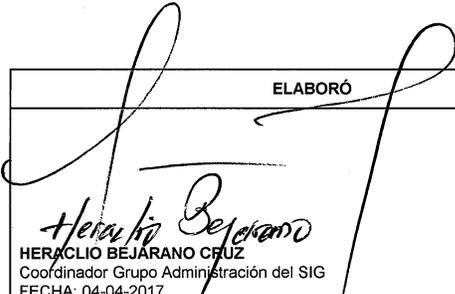


	<b>DOCUMENTO ESTRATÉGICO</b>	VERSIÓN 8
	<b>Política de Administración del Riesgo</b>	<b>DE-DEI-05</b> FECHA EDICIÓN 04-04-2017

# POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

ELABORÓ	APROBÓ
 <b>HERACLIO BEJARANO CRUZ</b> Coordinador Grupo Administración del SIG FECHA: 04-04-2017	 <b>ALEJANDRA PAEZ OSORIO</b> Secretaria General FECHA: 04-04-2017

*Handwritten mark*

	<b>DOCUMENTO ESTRATÉGICO</b>	VERSIÓN 8
	<b>Política de Administración del Riesgo</b>	<b>DE-DEI-05</b>
		FECHA EDICIÓN 04-04-2017

## CONTENIDO

1.	Objetivo .....	3
2.	Objetivos Específicos .....	3
3.	Lineamientos de la Política de Administración del Riesgo .....	3
4.	Historial de cambios .....	6



 <b>MINAGRICULTURA</b>	<b>DOCUMENTO ESTRATÉGICO</b>	<b>VERSIÓN</b> 8
	<b>Política de Administración del Riesgo</b>	<b>DE-DEI-05</b>
		<b>FECHA EDICIÓN</b> 04-04-2017

### 1. OBJETIVO

La política de Administración del Riesgo del Ministerio de Agricultura y Desarrollo Rural, tiene como propósito orientar las acciones que conduzcan a disminuir la vulnerabilidad de los procesos y procedimientos frente a situaciones que puedan interferir en el cumplimiento de sus funciones y objetivos institucionales.

### 2. OBJETIVOS ESPECÍFICOS

1. Identificar las posibles situaciones que generen riesgos en los procesos y procedimientos del Ministerio de Agricultura y Desarrollo Rural.
2. Reducir la vulnerabilidad y fortalecer la prevención y mitigación de los efectos de los riesgos.
3. Establecer actividades de control de manera conjunta con los líderes de los procesos, de acuerdo al direccionamiento estratégico de la Entidad.
4. Evitar que se creen situaciones de crisis en el Ministerio.
5. Proteger los recursos del Ministerio, resguardándolos contra la materialización de riesgos.

### 3. 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) Relacionados con las estrategias para establecer cómo se desarrolla la política, a corto, mediano y largo plazo.**

- 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.
- 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.
- 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.
- 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.
- 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).




	<b>DOCUMENTO ESTRATÉGICO</b>	VERSIÓN 8
	<b>Política de Administración del Riesgo</b>	<b>DE-DEI-05</b>
		FECHA EDICIÓN 04-04-2017

- 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.
- 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.
- 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.
- 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.

Para los riesgos de corrupción se toman las opciones “evitar el riesgo” ó “reducir el riesgo”.

**b) Relacionados con los riesgos que se van a controlar.**

- Los riesgos identificados en cada uno de los procesos se deben mantener controlados, por lo tanto los responsables de los procesos deben implementar los controles establecidos en los mapas de riesgos y tomar las acciones necesarias para evitar que los riesgos se materialicen.
- 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”.



	<b>DOCUMENTO ESTRATÉGICO</b>	VERSIÓN 8
	<b>Política de Administración del Riesgo</b>	<b>DE-DEI-05</b>
		FECHA EDICIÓN 04-04-2017

- 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.

**c) Relacionados con las acciones a desarrollar de forma permanente**

- 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.
- Los responsables de los procesos deben mantener las evidencias de la aplicación de los controles definidos para los riesgos identificados.
- Para los riesgos de corrupción los responsables de los procesos deben mantener identificadas las causas de los riesgos y que estas sean pertinentes con 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.

**d) Relacionados con el seguimiento y evaluación a la implementación y efectividad de las políticas.**

- La Oficina de Control Interno es responsable de realizar el seguimiento y evaluación a la implementación de los mapas de riesgos, definidos por los responsables de los procesos, acorde con la planeación establecida. 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"
- 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 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 Desarrollo Administrativo.



 MINAGRICULTURA	<b>DOCUMENTO ESTRATÉGICO</b>	VERSIÓN 8
	<b>Política de Administración del Riesgo</b>	<b>DE-DEI-05</b>
		FECHA EDICIÓN 04-04-2017

- Los responsables de los procesos que incurran en incumplimiento de los lineamientos de esta política, deberán adelantar acciones correctivas, que permitan eliminar la causa del incumplimiento. De ser reiterativa esta situación, se presentará a consideración del Comité Institucional de Desarrollo Administrativo, para que tome las decisiones pertinentes.

#### 4. 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).
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".



Proyecto: Heraclio Bejarano Cruz  
Coordinador Grupo Administración del SIG