POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

ELABORÓ	APROBÓ
HERACLIO BEJARANO CRUZ Coordinador Grupo Administración del SIG FECHA: 20-12-2019	ANA MARÍA LÓPEZ HERNÁNDEZ Secretaria General FECHA: 20-12-2019

CONTENIDO

1. OBJETIVO

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 frente a situaciones que puedan interferir en el cumplimiento de sus funciones y objetivos institucionales, con el propósito de llevar los riesgos identificados a niveles aceptables.

2. OBJETIVOS ESPECÍFICOS

1. Establecer el contexto externo e interno 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, legales 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.

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.

4. TÉRMINOS Y DEFINICIONES

- **RIESGO**: Posibilidad de ocurrencia de toda aquella situación que pueda tener impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad e impacto.
- **GESTION DE RIESGOS**: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **VALORACIÓN DEL RIESGO**: Análisis frente a la probabilidad de ocurrencia del riesgo y el nivel de impacto, con el objetivo de estimar la zona de riesgo inicial.
- **NIVEL DE RIESGO**: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación del impacto y su probabilidad.
- **CONTROL**: Medida que reduce el impacto o probabilidad del riesgo.
- **RIESGO RESIDUAL**: Riesgo remanente después del tratamiento del riesgo.

5. LINEAMIENTOS DE LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

El Ministerio de Agricultura y Desarrollo Rural establece las siguientes directrices a aplicar en la identificación, evaluación y tratamiento de los riesgos asociados a la gestión de sus procesos definidos en el Sistema Integrado de Gestión - SIG:

a) La metodología a utilizar.

- ❑ Se toma como metodología para la evaluación y valoración de los riesgos, los criterios establecidos en las guías "para la administración del riesgo y el diseño de controles en entidades públicas" del

Departamento Administrativo de la Función Pública - DAFP y "para la gestión del riesgo de corrupción", emitida por la Secretaria de Transparencia de la Presidencia de la Republica.

- ❑ La información de análisis de los riesgos para cada uno de los procesos es registrada en el formato "mapa de riesgos" (F01-PR-SIG-05) y se realiza su validación de acuerdo con lo establecido en el procedimiento "Gestión del Riesgo (PR-SIG-05)".

b) Directrices sobre los factores de riesgos estratégicos utilizados para realizar el análisis y establecimiento del contexto

El establecer el contexto es la parte más importante para identificar un riesgo debido a que enmarca de forma más clara las posibles debilidades o amenazas a que pueden estar expuestos los procesos de la entidad y de esta forma es más fácil analizar y llegar a concluir los riesgos que pueden interferir en el cumplimiento de sus objetivos. Para el análisis del contexto tenga en cuenta lo siguiente:

- ❑ Para los riesgos institucionales y de seguridad de la información identifique en cada proceso las posibles debilidades o amenazas sobre que pueden generar los riesgos, revisando los siguientes factores:

CONTEXTO	FACTOR	POSIBLES EVENTOS (DEBILIDADES O AMENAZAS) APLICABLES A LOS RIESGOS INSTITUCIONALES Y SEGURIDAD DE LA INFORMACION
Externo	Políticos	▪ Decisiones administrativas orientadas por compromisos de orden nacional. ▪ Intereses políticos que inducen a decisiones administrativas, para el establecimiento del marco legal que orienta la política agropecuaria. ▪ Decisiones enmarcadas dentro de los Acuerdos de Paz ▪ cambios de gobierno.
	Económicos y financieros	▪ Congelamiento o reducción del presupuesto sectorial ▪ Fluctuación en las tasas de cambio ▪ Políticas internacionales que fijan compromisos y otras orientaciones. ▪ Fluctuación en la demanda.
	Sociales	▪ Prácticas de conductas de acceso fraudulento o interferencia de terceros a los productos ofrecidos por la entidad. ▪ Información presentada para acceder a los productos en forma incompleta o con errores, que obliguen a postergar los tiempos para subsanar.
	Medioambientales	▪ Fenómenos naturales y/o catástrofes naturales, pueden afectar el normal desarrollo e implementación de la política sectorial. ▪ Fenómenos naturales y/o catástrofes naturales, pueden dañar los archivos o afectar la salud de las personas que laboran en las instalaciones del Ministerio.
	Tecnológico	▪ Aumento de los ataques informáticos relacionados con secuestro de información. ▪ Nuevas estrategias gubernamentales en materia de seguridad informática y ciberseguridad ▪ Apropiación de nuevas tecnologías.
	Legales y reglamentarios	▪ Legislación obsoleta. ▪ Falta de normatividad o normatividad confusa.

CONTEXTO	FACTOR	POSIBLES EVENTOS (DEBILIDADES O AMENAZAS) APLICABLES A LOS RIESGOS INSTITUCIONALES Y SEGURIDAD DE LA INFORMACION
Interno	Financieros	▪ Falta de recursos para infraestructura o para ampliar su capacidad.
	Personal	▪ Conocimiento y aplicabilidad del Sistema de Integrado de Gestión ▪ Desconocimiento de la normatividad aplicable ▪ Falta de planeación y directrices
	Procesos	▪ Demoras en los trámites administrativos dentro de los diferentes procesos ▪ Algunos procesos no cuentan con el personal suficiente para desarrollar las actividades programadas. ▪ Deficiencia en la Planeación y planes de acción ▪ Falta de rigurosidad en los seguimientos a la planeación ▪ Falta de conocimiento de los documentos del SIG. ▪ Control en la oportunidad de respuesta a las peticiones, quejas y reclamos.
	Tecnología	▪ Fallas en los mecanismos de Seguridad informática. ▪ Fallas tecnológicas en los equipos ▪ Baja cultura en aspectos de seguridad de la información. ▪ Planeación deficiente en cambios de infraestructura
	Estratégicos	▪ Dificultad para trabajar en equipo ▪ Directrices poco claras o inexistentes ▪ Planeación con compromisos de difícil cumplimiento.
	Comunicación interna	▪ Canales de comunicación no utilizados o con fallas que impiden realizar la comunicación. ▪ Información deficiente
Proceso	Diseño del proceso	▪ Objetivo y alcance del proceso poco claros.
	Interacciones con otros procesos	▪ Falta de claridad en la interacción con otros procesos en lo relacionado con productos o insumos a entregar o recibir.
	Transversalidad	▪ Falta de claridad en las directrices para darle el manejo cuando los temas se desarrollan en más de un proceso.
	Procedimientos asociados	▪ No tener un responsable asociado a las actividades a adelantar o que este no sea claro. ▪ Deficiencia en la
	Responsables del proceso	▪ No existir responsable por los temas. ▪ Omisión en la responsabilidad del tema
	Comunicación entre los procesos	▪ Poca efectividad en la transmisión de la información
	Activos de seguridad digital del proceso	▪ Debilidades en la disponibilidad, confidencialidad e integridad de la información que este contenida en forma electrónica, en aplicativos, físico u otros y que indispensables para la gestión de los procesos.

Tabla 1. Factores aplicables para la evaluación del contexto en la identificación de los riesgos y causas

Los anteriores factores son de orientación para poder identificar de manera más precisa el riesgo y sus causas, así mismo tener en cuenta que en un riesgo puede verse reflejados uno o varios factores (no se requieren que todos los factores se vean reflejados en un riesgo).

- ❑ Para los riesgos de corrupción se verifica dentro de los procesos la presencia de algunas de las debilidades que se relacionan a continuación:

ACTIVIDADES	SITUACIONES QUE PUEDEN DAR ORIGEN A UN RIESGO DE CORRUPCION
Direccionamiento estratégico (Alta Dirección)	Concentración de autoridad o exceso de poder.
	Extralimitación de funciones.
	Ausencia de canales de comunicación.
	Amiguismo y clientelismo.
Financiero (está relacionado con áreas de planeación y presupuesto).	Inclusión de gastos no autorizados.
	Inversiones de dineros públicos en entidades de dudosa solidez financiera, a cambio de beneficios indebidos para servidores públicos encargados de su administración.
	Inexistencia de registros auxiliares que permitan identificar y controlar los rubros de inversión.
	Inexistencia de archivos contables.
	Afectar rubros que no corresponden con el objeto del gasto en beneficio propio o a cambio de una retribución económica.
De contratación (como proceso o bien los procedimientos ligados a este).	Estudios previos o de factibilidad deficientes.
	Estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación. (Estableciendo necesidades inexistentes o aspectos que benefician a una firma en particular).
	Pliegos de condiciones hechos a la medida de una firma en particular.
	Disposiciones establecidas en los pliegos de condiciones que dirigen los procesos hacia un grupo en particular. (Ej. media geométrica).
	Visitas obligatorias establecidas en el pliego de condiciones que restringen la participación.
	Adendas que cambian condiciones generales del proceso para favorecer a grupos determinados.
	Urgencia manifiesta inexistente.
	Otorgar labores de supervisión a personal sin conocimiento para ello.
	Concentrar las labores de supervisión en poco personal.
	Contratar con compañías de papel que no cuentan con experiencia.
De información y documentación	Ausencia o debilidad de medidas y/o políticas de conflictos de interés.
	Concentración de información de determinadas actividades o procesos en una persona.
	Ausencia de sistemas de información, que pueden facilitar el acceso a información y su posible manipulación o adulteración.
	Ocultar la información considerada pública para los usuarios.
	Ausencia o debilidad de canales de comunicación
	Incumplimiento de la Ley 1712 de 2014.

ACTIVIDADES	SITUACIONES QUE PUEDEN DAR ORIGEN A UN RIESGO DE CORRUPCION
De investigación y sanción	Ausencia o debilidad de canales de comunicación.
	Dilatar el proceso para lograr el vencimiento de términos o la prescripción del mismo.
	Desconocimiento de la ley, mediante interpretaciones subjetivas de las normas vigentes para evitar o postergar su aplicación.
	Exceder las facultades legales en los fallos.
De trámites y/o servicios internos y externos	Cobros asociados al trámite.
	Influencia de tramitadores
	Tráfico de influencias: (amiguismo, persona influyente).
De reconocimiento de un derecho (expedición de licencias y/o permisos).	Falta de procedimientos claros para el trámite.
	Imposibilitar el otorgamiento de una licencia o permiso.
	Ofrecer beneficios económicos para aligerar la expedición o para amañar la misma.
	Tráfico de influencias: (amiguismo, persona influyente).

Tabla 2. Relación de actividades y posibles debilidades que pueden originar riesgos de corrupción

c) Lineamientos a aplicar en la elaboración o modificación de las matrices de riesgos en el formato "mapa de riesgos" (F01-PR-SIG-05).

La elaboración o modificación de las matrices de riesgos, se realiza en cuatro fases: identificación del riesgo, valoración del riesgo, identificación de controles y valoración del riesgo residual. A continuación, se define los criterios a tener en cuenta en cada una de estas fases:

Fase identificación del riesgo:

Basados en la revisión realizada en cada uno de los factores y las posibles amenazas o debilidades que le son aplicables al proceso, se procede a identificar los riesgos, teniendo en cuenta lo siguiente:

- Para la redacción de los riesgos se puede tomar como guía las técnicas definidas por el Departamento Administrativo de la Función Pública - DAFP en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" en el numeral "2.2.1. Técnicas para la redacción de riesgos". Se puede descargar en la página del DAFP, en el siguiente link: https://www.funcionpublica.gov.co/documents/418548/34150781/Gu%C3%ADa+para+la+administraci%C3%B3n+del+riesgo+y+el+dise%C3%B1o+de+controles+en+entidades+p%C3%BAblicas+-+Riesgos+de+gesti%C3%B3n%2C+corrupci%C3%B3n+y+seguridad+digital+-+Versi%C3%B3n+4+-+Octubre+de+2018.pdf/68d324dd-55c5-11e0-9f37-2e5516b48a87?t=1542208781163.

- Para la identificación de los riesgos de "seguridad de la información" las debilidades y amenazas se analizan sobre los activos de información identificados para los procesos en el formato "inventario de activos de información F01-PR-GST-10". En caso de no estar en esta relación se relaciona en la matriz de riesgo y posteriormente se actualiza este inventario, de acuerdo a lo establecido en el procedimiento "clasificación y etiquetado de la información PR-GST-10".

- Es posible que los riesgos de corrupción no estén presentes en todos los procesos, pero es obligatorio identificarlos en aquellos procesos donde se den manejo de recursos o decisiones sobre la contratación y seguimientos de los contratos formalizados.

Nota: Es importante resaltar que los riesgos identificados para los procesos y registrados en el formato "mapa de riesgos" (F01-PR-SIG-05), se encuentran acordes a lo dispuesto en el numeral 6 de la norma ISO 9001:2015 e ISO 27001:2013.

- **Fase valoración del riesgo:**

Los riesgos identificados en la fase anterior se deben valorar en función de la probabilidad y el impacto, para ello se tiene en cuenta lo siguiente:

Probabilidad

- Para la valoración de la probabilidad se selecciona el valor teniendo como referencia los siguientes criterios:

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	**Probable**	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	**Posible**	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	**Improbable**	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	**Rara vez**	El evento puede ocurrir solo en Circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

Tabla 3. Criterios de evaluación de la probabilidad

- Al momento que se aplique la valoración cuantitativa inherente para los riesgos de corrupción, la probabilidad se califica seleccionando opción 1 (rara vez) al 5 (Casi Seguro).

Impacto:

Para valorar el impacto se asignan valores así: 1- Insignificante;2- Menor;3- Moderado;4- Mayor;5- Catastrófico. Cada uno de los estos valores son asignados de acuerdo con los siguientes criterios:

- Para la valoración del impacto en los riesgos institucionales se selecciona el valor de acuerdo con los criterios (cualitativo o cuantitativo) definidos a continuación:

NIVEL IMPACTO	VALORACION (CONSECUENCIAS) CUANTITATIVA	VALORACION (CONSECUENCIAS) CUALITATIVA

NIVEL IMPACTO	VALORACION (CONSECUENCIAS) CUANTITATIVA	VALORACION (CONSECUENCIAS) CUALITATIVA
5- CATASTRÓFICO	• Impacto que afecte la ejecución presupuestal en un valor ≥50%. • Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50%. • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	• 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.
4- MAYOR	• Impacto que afecte la ejecución presupuestal en un valor ≥20%. • Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20%. • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	• 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 del 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.
3- MODERADO	• Impacto que afecte la ejecución presupuestal en un valor ≥5%. • Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el pre- supuesto total de la entidad en un valor ≥5%. • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad.	• 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.

NIVEL IMPACTO	VALORACION (CONSECUENCIAS) CUANTITATIVA	VALORACION (CONSECUENCIAS) CUALITATIVA
2- MENOR	• Impacto que afecte la ejecución presupuestal en un valor ≥1%. • Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%. • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el pre- supuesto total de la entidad en un valor ≥1%. • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la entidad.	• 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.
1- INSIGNIFICANTE	• Impacto que afecte la ejecución presupuestal en un valor ≥0,5%. • Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%. • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5%. • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la entidad.	• 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 4. Criterios de evaluación impacto para riesgos institucionales

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

NIVEL IMPACTO	VALORACION (CONSECUENCIAS) CUANTITATIVA	VALORACION (CONSECUENCIAS) CUALITATIVA
1- INSIGNIFICANTE	• Afectación ≥X% de la población. • Afectación ≥X% del presupuesto anual de la entidad. • No hay afectación medioambiental.	• Sin afectación de la integridad. • Sin afectación de la disponibilidad. • Sin afectación de la confidencialidad.
2- MENOR	• Afectación ≥X% de la población. • Afectación ≥X% del presupuesto anual de la entidad. • Afectación leve del medio ambiente requiere de ≥X días de recuperación.	• Afectación leve de la integridad. • Afectación leve de la disponibilidad. • Afectación leve de la confidencialidad.

NIVEL IMPACTO	VALORACION (CONSECUENCIAS) CUANTITATIVA	VALORACION (CONSECUENCIAS) CUALITATIVA
3- MODERADO	• Afectación ≥X% de la población. • Afectación ≥X% del presupuesto anual de la entidad. • Afectación leve del medio ambiente requiere de ≥X semanas de recuperación.	• Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. • Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. • Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.
4- MAYOR	• Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. • Afectación importante del medio ambiente que requiere de ≥X meses de recuperación.	• Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. • Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. • Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
5-CATASTRÓFICO	• Afectación ≥X% de la población. • Afectación ≥X% del presupuesto anual de la entidad. • Afectación muy grave del medio ambiente que requiere de ≥X años de recuperación.	• Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. • Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. • Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.

Tabla 5. Criterios para evaluar el impacto en los riesgos de seguridad de la información

- ❑ Para los riesgos de corrupción el impacto se puede calificar como moderado (3), mayor (4) o catastrófico (5), haciendo uso del siguiente cuestionario de ayuda:

PREGUNTA	RESPUESTA	
	SÍ	NO
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,		

servicios o recursos públicos?		
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?		
19 ¿Generar daño ambiental?		
Responder afirmativamente de UNA a CINCO preguntas(s) genera un impacto moderado.		
Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor.		
Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.		
MODERADO: Genera medianas consecuencias sobre la entidad MAYOR: Genera altas consecuencias sobre la entidad. CATASTRÓFICO: Genera consecuencias desastrosas para la entidad		

Tabla 6. Cuestionario aplicable para establecer el impacto de los riesgos de corrupción

- Las valoraciones realizadas de la probabilidad y el impacto para los riesgos identificados, se les determina la zona en que queda valorada la exposición de la entidad con respecto al riesgo, las cuales pueden ser: Extremo, alto, moderado y bajo. Las zonas son identificadas para cada riesgo de acuerdo con la siguiente tabla:

PROBABILIDAD	IMPACTO				
	1- Insignificante	2- Menor	3- Moderado	4- Mayor	5- Catastrófico
5- Casi seguro	A	A	E	E	E
4- Probable	M	A	A	E	E
3- Posible	B	M	A	E	E
2- Improbable	B	B	M	A	E
1- Rara vez	B	B	M	A	E

zonas
Extremo (E)
Alto (A)
Moderado (M)
Bajo (B)

Tabla 7. Matriz de evaluación y calificación de riesgos

- **Fase identificación de controles**

- Para cada causa establecida en la identificación del riesgo se le establece un control. Si el control es el mismo para varias causas se repite en cada fila la información del mismo control.

- Cuando se hace referencia a un documento o política como control debe especificarse la actividad que contiene el documento y que es tenido en cuenta como control. En caso de ser todo el documento debe especificarse que el control hace referencia es a la aplicación de todo definido en este.

- ❑ A cada control establecido se le debe definir: periodicidad, propósito del control, forma de realización del control, forma de proceder cuando hay desviaciones en la ejecución del control, evidencia de ejecución del control. Esta información es definida por el responsable del proceso.

- ❑ Los controles para el tratamiento de los riesgos "Seguridad de la información" son seleccionados con el acompañamiento de la Oficina de Tecnologías de la Información y las Comunicaciones, de acuerdo con 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.

- **Fase valoración del riesgo residual**

- ❑ Esta valoración es realizada por los profesionales del Grupo Administración del SIG, una vez los responsables de los procesos hayan identificado los controles, para lo cual, se le realiza una estimación sobre los siguientes aspectos:

  i. Diseño del control
  ii. Ejecución del control
  iii. Solidez del control

  Evaluación de Diseño: Para realizar esta valoración se debe aplicar la siguiente tabla del control, para lo cual, se da respuesta a cada una de las siguientes preguntas, asignando el valor de la tabla por cada criterio, la sumatoria de todos los criterios determina la evaluación al diseño.

CRITERIO DE EVALUACIÓN	PREGUNTA	OPCIÓN DE RESPUESTA	VALOR ASIGNADO SEGÚN RESPUESTA
1.1 Asignación del responsable	¿Existe un responsable asignado a la ejecución del control?	Asignado	15
		No Asignado	0
1.2 Segregación y autoridad del responsable.	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado	15
		Inadecuado	0
2. Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna	15
		Inoportuna	0
3. Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, ejemplo Verificar, Validar, Cotejar, Comparar, Revisar, etc.?	Prevenir	15
		Detectar	10
		No es un control	0
4. Cómo se realiza la actividad de control.	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	Confiable	15
		No confiable	0

CRITERIO DE EVALUACIÓN	PREGUNTA	OPCIÓN DE RESPUESTA	VALOR ASIGNADO SEGÚN RESPUESTA
5. Qué pasa con las observaciones o desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven oportunamente	15
		No se investigan y resuelven oportunamente	0
6. Evidencia de la ejecución del control.	¿Se deja evidencia o rastro de la ejecución del control, que permita a cualquier tercero con la evidencia, llegar a la misma conclusión?	Completa	10
		Incompleta	5
		No existe	0
Evaluación de los resultados del diseño del control: **Fuerte**: Para calificación entre 96 y 100 **Moderado**: Calificación entre 86 y 95 **Débil**: Calificación entre 0 y 85			

Tabla 8. Criterios para evaluar el diseño de los controles

- **Evaluación de la ejecución del control:** Una vez realizada la evaluación al diseño, se debe ubicar la calificación obtenida en la tabla que se registra a continuación y con base en las evidencias entregadas por el Líder del Proceso frente a la ejecución de los controles establecidos para cada riesgo, se clasificará de acuerdo con los siguientes criterios:

CALIFICACION DADA EN EL DISEÑO (INDIVIDUAL POR CONTROL)	OPCIONES DE RESPUESTA A SI EL CONTROL SE EJECUTA DE MANERA CONSISTENTE POR LOS RESPONSABLES (EJECUCIÓN)
"Fuerte" calificación entre 96 y 100"	Fuerte (siempre se ejecuta)
	Moderado (algunas veces)
	Débil (no se ejecuta)
"Moderado" calificación entre 86 y 95	Fuerte (siempre se ejecuta)
	Moderado (algunas veces)
	Débil (no se ejecuta)
"Débil" calificación entre 0 y 85	Fuerte (siempre se ejecuta)
	Moderado (algunas veces)
	Débil (no se ejecuta)

Tabla 9. Criterios para evaluar la ejecución de los controles

- **Evaluación de la solidez del control:** De acuerdo con las evaluaciones dadas para el diseño y la ejecución, se evalúa la solidez, de acuerdo con los siguientes criterios:

CALIFICACION DADA EN EL DISEÑO (INDIVIDUAL POR CONTROL)	OPCIONES DE RESPUESTA A SI EL CONTROL SE EJECUTA DE MANERA CONSISTENTE POR LOS RESPONSABLES (EJECUCIÓN)	VALORACION INDIVIDUAL POR CONTROL	
		Evaluación	Valor
"Fuerte" calificación entre 96 y	Fuerte (siempre se ejecuta)	Fuerte	100

CALIFICACION DADA EN EL DISEÑO (INDIVIDUAL POR CONTROL)	OPCIONES DE RESPUESTA A SI EL CONTROL SE EJECUTA DE MANERA CONSISTENTE POR LOS RESPONSABLES (EJECUCIÓN)	VALORACION INDIVIDUAL POR CONTROL	
		Evaluación	Valor
100"	Moderado (algunas veces)	Moderado	50
	Débil (no se ejecuta)	Débil	0
"Moderado" calificación entre 86 y 95	Fuerte (siempre se ejecuta)	Moderado	50
	Moderado (algunas veces)	Moderado	50
	Débil (no se ejecuta)	Débil	0
"Débil" calificación entre 0 y 85	Fuerte (siempre se ejecuta)	Débil	0
	Moderado (algunas veces)	Débil	0
	Débil (no se ejecuta)	Débil	0

Tabla 10. Criterios para evaluar la solidez de los controles

Una vez evaluado cada control de manera individual se calcula el promedio aritmético simple del conjunto de controles definidos para cada riesgo y se determina el valor final de la solidez y se clasifica de acuerdo a los siguientes rangos:

Fuerte: El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100.
Moderado: El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre 50 y 99.
Débil: El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50.

- El cálculo del riesgo residual se efectúa de acuerdo con la calificación dada a la solidez del conjunto de los controles definidos para el respectivo riesgo, de acuerdo con el siguiente criterio:

VALORACION DADA A LA SOLIDEZ DEL CONJUNTO DE CONTROLES	CONTROLES AYUDAN A DISMINUIR LA PROBABILIDAD	CONTROLES AYUDAN A DISMINUIR EL IMPACTO	ESPACIOS A DESPLAZAR	
			en el eje de la probabilidad	en el eje de impacto
Fuerte	directamente	directamente	2	2
Fuerte	directamente	indirectamente	2	1
Fuerte	directamente	no disminuye	2	0
Fuerte	no disminuye	directamente	0	2
Moderado	directamente	directamente	1	1
Moderado	directamente	Indirectamente	1	0
Moderado	directamente	no disminuye	1	0
Moderado	no disminuye	directamente	0	1

Tabla 11. Criterios para evaluar el riesgo residual

Una vez calculado el riesgo residual, se actualiza en el formato "MAPA DE RIESGOS" (F01-PR-SIG-05), determinando la zona residual en la que queda la nueva valoración del riesgo en función de la probabilidad e impacto.

d) Niveles de aceptación de riesgos para la entidad y su forma de manejo

- El Ministerio de Agricultura y Desarrollo Rural establece como riesgos con nivel aceptable aquellos cuyas zonas residuales queden en "bajo" o "Moderado".

- Las opciones de tratamiento de riesgos para los riesgos residuales son:
  Aceptar
  Reducir
  Evitar
  Compartir

  A su turno, los riesgos de corrupción, debe tratarse a través de la formulación de un Plan de Contingencia.

- La opción de manejo se determinar con base en los siguientes criterios:

Opción de tratamiento de riesgo	Zona residual del riesgo a los que aplica	Tipo de riesgos a lo que aplica	Forma de manejo
Aceptar	▪ Bajo ▪ Moderado	▪ Institucionales ▪ Seguridad de la información	Se aplica los controles como se definieron y se reevalúa cuando se materializa.
Reducir	▪ Alto ▪ Extremo	▪ Corrupción ▪ Institucionales ▪ Seguridad de la información	Plan de tratamiento de riesgos
Evitar	▪ Cualquier zona	▪ Corrupción ▪ Institucionales ▪ Seguridad de la información	Plan de tratamiento de riesgos
Compartir	▪ Cualquier zona (cuando contempla como control pólizas o delegación de la función)	▪ Corrupción ▪ Institucionales ▪ Seguridad de la información	Plan de tratamiento de riesgos
Acción de contingencia	▪ Cualquier zona	▪ Corrupción	Se debe establecer el plan de contingencia, en caso de materializarse el riesgo y registrarlo en el plan de tratamiento de riesgos.
	▪ Extremo	▪ Institucionales	Plan de tratamiento de riesgos

Tabla 12. Criterios para seleccionar opciones de manejo del riesgo

- Cuando la forma de manejo sea establecer un Plan de Tratamiento de Riesgos, el Líder del Proceso, deberá garantizar que el mismo se establezca y cumpla oportunamente.

e) Periodicidad para el monitoreo, la revisión y seguimiento de los riesgos

- 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 con el apoyo del Grupo Administración del SIG.

- Los responsables de los procesos deben verificar que los riesgos se encuentren actualizados, se apliquen los controles definidos, se efectúen las acciones del plan de tratamiento de riesgos y se monitoreen los mismos, de lo cual se dejará constancia en el anexo del Formato "MAPA DE RIESGOS" (F01-PR-SIG-05).

- 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" en coordinación con el Grupo Administración del SIG.

- 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 Control Interno.

f) Niveles de responsabilidad en relación con la gestión los riesgos:

- Los responsables de los procesos deben identificar las situaciones que puedan afectar el desarrollo de las actividades de los procesos o el logro de los objetivos propuestos y establecer los controles necesarios y su pertinencia para evitar que los riesgo se materialicen, los cuales deben ser formalizados y comunicados al Proceso Administración del Sistema Integrado de Gestión, a efectos de mantener actualizados los mapas de riesgos.

- 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 garantizar los recursos (físicos, financieros y de 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.

- Los responsables de los procesos deben adelantar las acciones preventivas, correctivas, o mejora ante las situaciones detectadas por el autocontrol o por la Oficina de Control Interno, cuando así se requiera, o cuando se materialice un riesgo, 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 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.

6. 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 con 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 con la guía "para la administración del riesgo", del Departamento Administrativo de la Función-DAFP (versión 3, diciembre de 2014).
28-11-2019	10	Se ajustó la estructura general del documento de acuerdo con la *"Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas"*, del Departamento Administrativo de la Función-DAFP (versión 4, octubre de 2018), ISO 9001:2015 e ISO 27001:2013

Proyectó: Heraclio Bejarano Cruz
Coordinador Grupo Administración del SIG