POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

ELABORÓ	APROBÓ
HERACLIO BEJARANO CRUZ Coordinador Grupo Administración del SIG Fecha: 27-05-2022	**MARTHA LUCIA RODRÍGUEZ LOZANO** Secretaria General Fecha: 27-05-2022

CONTENIDO

1. OBJETIVO

Definir los lineamientos de la política integral de gestión del riesgo en el Ministerio de Agricultura que conduzcan a disminuir la vulnerabilidad frente a situaciones que puedan interferir en el cumplimiento de sus funciones y objetivos estratégicos institucionales, con el propósito de llevar los riesgos identificados a niveles aceptables con un enfoque preventivo que permita la protección de los recursos, alcanzar mejores resultados y mejorar la prestación de servicios a sus usuarios.

2. ALCANCE

La Política de Administración del Riesgo aplica a todos los procesos del Sistema Integrado de Gestión del Ministerio de Agricultura y Desarrollo Rural, incluyendo en el caso particular para los riesgos de seguridad de información y terceros que suministren información para la gestión institucional.

3. TÉRMINOS Y DEFINICIONES

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

Riesgo de Seguridad de la Información: 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 27000).

Riesgo de Corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgo de Fraude: Acción de engaño intencional, que un servidor público o particular con funciones, públicas, realiza con el propósito de conseguir un beneficio o ventaja ilegal para sí mismo o para un tercero.

Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año**.**

Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Consecuencia: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Riesgo Inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.

Control: Medida que permite reducir o mitigar un riesgo.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados**.**

Integridad: Propiedad de exactitud y completitud.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas**.**

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo puede ser Probabilidad por Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

Tolerancia del riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad**.**

Capacidad de riesgo: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

Apetito de riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar**.**

Plan Anticorrupción y de Atención al Ciudadano: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

4. CONTEXTO DE LA ENTIDAD

5.1 Contexto Externo

La problemática por la que atraviesa el Sector Agropecuario y Rural, está estrictamente relacionada con la falta de rentabilidad en la mayoría de las actividades productivas, y en mayor desventaja para el pequeño y mediano productor, lo cual se deriva principalmente de la falta de productividad y competitividad, revaluación de la tasa real de cambio, aumento del ingreso percapita de los consumidores, desestimulando la inversión, distorsiones en los canales de comercialización, entre otros factores.

Los precarios ingresos que genera la población rural afectan notablemente su calidad de vida y el nivel de pobreza, la cual ha sido una condición medible en el sector rural que sirve como punto de referencia para observar la evolución del desarrollo y la equidad de la población; por lo anterior, al mantener la medición de este fenómeno social es posible realizar comparativos y hacer lecturas amplias de las dinámicas rurales.

La carencia de ingresos en la población afecta de forma negativa las cinco dimensiones que dan lugar al Índice de pobreza multimensional (IPM), como son sus condiciones educativas, de la niñez y juventud, de salud, de la vivienda y los servicios públicos. De acuerdo con los resultados del 3er Censo Nacional Agropecuario, el 45,7 % de las personas residentes del área rural dispersa censada se encuentra en condición de pobreza, equivalente a 2.344.668 personas.

Desde los inicios de la década del 90, por la falta de competitividad en la producción agropecuaria el País poco a poco se fue rezagando en el auto abastecimiento de producción agropecuaria y pesquera, atendiendo el consumo nacional cada vez con mayores importaciones, contribuyendo a un mayor déficit en la cuenta corriente. Hoy el 50 % de importaciones puede ser sustituido.

Persisten retos en el uso eficiente del suelo rural y la consolidación de cadenas de valor agroindustriales que permitan la transformación productiva del sector. Por un lado, existe sobreutilización y subutilización en el suelo del orden del 11,7% y 13,0%, respectivamente. Por otro lado, por cada km2 de tierra arable en Colombia se generaron USD 33.200 en 2013, lo que equivale al 19% de la productividad en los países de la OCDE. Estas dinámicas en el uso del suelo, asociadas a prácticas ineficientes de producción, impiden que el país aproveche plenamente su potencialidad agropecuaria y cuente con una mayor disponibilidad de alimentos.

En el 45,0% de las Unidades Agropecuarias (UA), los productores declaran realizar prácticas para mejorar suelos, y el 70,2% de las UA, los productores declaran haber aplicado fertilizantes químicos para mejorar los suelos, y el 46,5% de las UA se utilizan fertilizantes orgánicos. En el 52,2% de las UA, los productores declaran utilizar controles contra plagas, malezas y enfermedades, y de estas el 57,8% los productores declaran haber usado controles químicos. Así mismo, en el 53,0% de las UA se realizaron controles manuales.

El País aún posee una baja diversificación de la oferta exportadora: café, flores, banano y azúcar concentran el 80 % de las exportaciones agropecuarias, lo cual se deriva de la falta de competitividad, pero principalmente por falta de cumplimiento de estándares sanitarios y de inocuidad. En términos de infraestructura de vías y aeroportuarias para el acceso a los mercados, el 90% de las vías terciarias se encuentran en mal estado, de donde el 75 % de las zonas rurales, se encuentra a más de tres (3) horas de ciudades principales, lo cual afecta considerablemente los costos de transporte.

5.2 Contexto Interno

El Ministerio de Agricultura y Desarrollo Rural, es una entidad nacional, creada mediante la Ley 25 del 8 de octubre de 1913, regida por la Constitución Política y por las leyes de la República de Colombia.

Los artículos 58 y 59 de la Ley 489 de 1998, los Ministerios tienen entre sus objetivos primordiales "*La formulación y adopción de las políticas, planes generales, programas y proyectos del sector administrativo que dirigen*", y entre sus funciones está promover, de conformidad con los principios constitucionales, la participación de entidades en la prestación de servicios y actividades relacionados con su ámbito de competencia. Así mismo, de acuerdo con el artículo 3 de la Ley 1437 de 2011, las actuaciones administrativas se desarrollarán con arreglo a los principios de participación y coordinación, entre otros, y en virtud de este último principio "C*oncertarán sus actividades con las de otras instancias estatales en el cumplimiento de sus cometidos y en el reconocimiento de sus derechos a los particulares*".

La entidad ha mantenido la estructura organizacional definida en el Decreto 1985 de 2013, modificado por el decreto 1470 de 2018, que permitió la creación de 9 direcciones misionales, 2 viceministerios, 5 oficinas, secretaria general, 2 subdirecciones y el despacho del ministro. La estructura funcional de la entidad se ve reflejada en el organigrama, publicado en la página WEB, en el siguiente enlace: https://www.minagricultura.gov.co/ministerio/Paginas/Organigrama-Minagricultura.aspx

El Ministerio de Agricultura y Desarrollo Rural debe desarrollar los objetivos establecidos en el artículo 2 del Decreto 1985 de 2013, entre los cuales se encuentra "*Promover el desarrollo rural con enfoque territorial y el fortalecimiento de la productividad y competitividad de los productos agropecuarios, a través de acciones integrales que mejoren las condiciones de vida de los pobladores rurales, permitan el aprovechamiento sustentable de los recursos naturales, generen empleo y logren el crecimiento sostenido y equilibrado de las regiones", y "propiciar la articulación de las acciones institucionales en el medio rural de manera focalizada y sistemática, bajo principios de competitividad, equidad, sostenibilidad, multisectorialidad y descentralización, para el desarrollo socioeconómico del país*". En ese sentido, los numerales 1 y 3 del artículo 3 del Decreto 1985 de 2013 disponen como funciones del Ministerio de Agricultura y Desarrollo Rural "*Formular, dirigir, coordinar y evaluar la política relacionada con el desarrollo rural, agropecuario, pesquero y forestal en los temas de su competencia*", y "*Formular acciones para propiciar la articulación interinstitucional de las entidades del orden nacional y territorial que conlleven a la implementación de planes, programas y proyectos de desarrollo rural, y agropecuario con enfoque territorial*".

Institucionalmente se ha enfrentado a entornos donde exige el uso de tecnologías para lo cual la institución desde al año 2012 ha emprendido la estrategia del uso y aplicación de la tecnología en sus procesos administrativos, lo cual a su vez ha permitido que se presenten debilidades relacionadas con la obsolescencia de los equipos e infraestructura, deficiencia en los protocolos de seguridad de la información por la baja cultura por parte de los usuarios. Existen procesos internos que se realizan de manera manual donde no se puede tener información de manera oportuna para tomar decisiones a pesar de que esa información esta generada en forma física o en algunos documentos que están en los ordenadores de cada servidor.

Así mismo, a pesar que se tienen formalizados en los documentos del SIG las responsabilidades y obligaciones por parte de los servidores del Ministerio, aún persisten dificultades en el conocimiento y aplicación de los mismos, llevando a situaciones como falta de oportunidad en las respuesta de los PQRSD, falta de rigurosidad en los seguimientos a la planeación establecida, demoras en los tramites o entregas de los productos internos, falta de trabajo en equipo o planeación con compromisos de difícil cumplimiento. La mayoría de la información documentada está asociada a los procesos estratégicos, de

apoyo y los de evaluación; siendo los procesos misionales los que ofrecen dentro del SIG la menor cantidad de documentos que detallen la forma como realizan sus actividades,

El edificio Pedro A. López, es la sede central donde se desarrollan las actividades para los procesos, a excepción de control interno, gestión documental, almacén, atención y servicio al ciudadano; las cuales se desarrollan en el edificio BANCOL. Es importante destacar que debido a que las instalaciones de la sede central han estado desde el año 2016 sometido a un reforzamiento estructural y no han culminado estos trabajos por situaciones asociadas al hecho de ser un patrimonio histórico y cultural, estas instalaciones están expuestas a generar la materialización de los riesgos a la seguridad y salud de los servidores públicos.

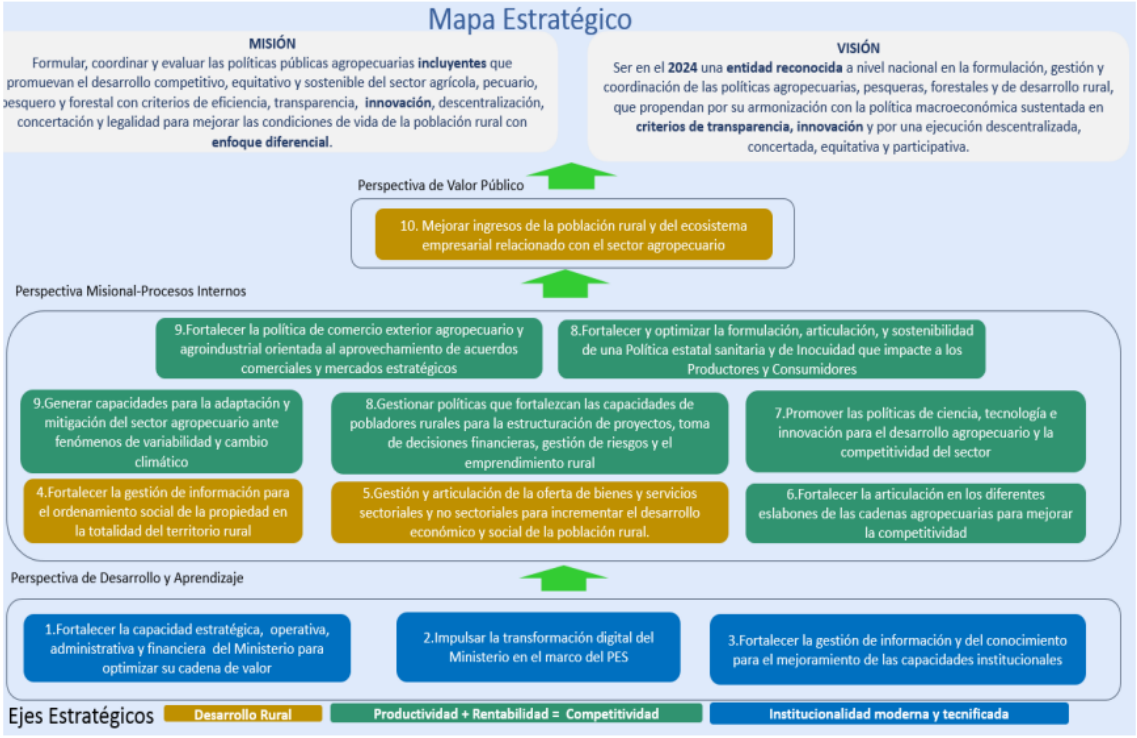
Los aspectos de la planeación estratégica a tener en cuenta en la identificación de los riesgos son los siguientes:

Misión: Formular, coordinar y evaluar las políticas públicas agropecuarias incluyentes que promueven el desarrollo competitivo, equitativo y sostenible del sector agrícola, pecuario, pesquero y forestal con criterios de eficiencia, transparencia, innovación, descentralización, concertación y legalidad para mejorar las condiciones de vida de la población rural con enfoque diferencial.

Visión: Ser en el 2024 una entidad reconocida a nivel nacional en la formulación, gestión y coordinación de las políticas agropecuarias, pesqueras, forestales y de desarrollo rural, que propendan por su armonización con la política macroeconómica sustentada en criterios de transparencia, innovación y por una ejecución descentralizada, concertada, equitativa y participativa.

Objetivos institucionales:

1. Mejorar el ingreso de la población rural
2. Fortalecer la gestión de información para el ordenamiento social de la propiedad en la totalidad del territorio rural
3. Gestionar y articular la oferta de bienes y servicios sectoriales y no sectoriales para incrementar el desarrollo económico y social de la población rural
4. Fortalecer la articulación en los diferentes eslabones de las cadenas agropecuarias para mejorar la competitividad
5. Promover las políticas de ciencia, tecnología e innovación para el desarrollo agropecuario y la competitividad del sector
6. Generar capacidades para la adaptación y mitigación del sector agropecuario ante fenómenos de variabilidad y cambio climático
7. Gestionar políticas que fortalezcan las capacidades de pobladores rurales para la estructuración de proyectos, toma de decisiones financieras, gestión de riesgos y el emprendimiento rural
8. Fortalecer y optimizar la formulación, articulación, aplicación y sostenibilidad de una Política estatal sanitaria y de Inocuidad que impacte a los Productores y Consumidores
9. Fortalecer la capacidad estratégica, operativa, administrativa y financiera del Ministerio para optimizar su cadena de valor
10. Fortalecer la gestión de información y del conocimiento para el mejoramiento de las capacidades institucionales
11. Impulsar la transformación digital del sector agropecuario y rural



5. LINEAMIENTOS DE LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

Para la construcción y la implementación de la presente política, se tomaron como referencia los lineamientos del Departamento Administrativo de la Función Pública – DAFP, establecidos mediante la "Guía de la Administración del Riesgo y el Diseño de Controles en las Entidades Públicas versión 5" – 2020, la norma técnica NTC ISO 31000:2018, los principios y directrices de los riesgos de seguridad digital y el Modelo de Seguridad y Privacidad de la Información – Mintic – ISO/IEC 27001:2013 y los lineamentos emitidos por la Secretaria de Transparencia de la Republica, en materia de riesgos de corrupción.

Se toma como metodología para la construcción, evaluación y valoración de los riesgos de gestión, corrupción y seguridad de la información, la mencionada Guía para la Administración del Riesgo, la cual hace parte integral de este documento.

La información de la construcción, evaluación y valoración de los riesgos para cada uno de los procesos se registrará en el formato denominado Mapa de Riesgos - F01-PR-SIG-05 y se realiza su validación de acuerdo con lo establecido en el procedimiento de Gestión del Riesgo - PR-SIG-05.

5.1 Niveles de Responsabilidad

A través de la siguiente matriz se definen la responsabilidad frente al riesgo, así:

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
Estratégica	Alta Dirección. Comité Institucional de Coordinador de Control Interno – CICCI	• Establecer y aprobar la Política de Administración del Riesgo la cual incluye los niveles de responsabilidad y autoridad. • Definir y hacer seguimiento a los niveles de aceptación. • Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles. • Realimentar al Comité Institucional de Gestión y Desempeño sobre los ajustes que se deban hacer frente a la gestión del riesgo. • Evaluar el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento de este, acorde con la información generada por parte de las instancias de la 2ª línea identificadas y la actividad de control definida que materializa la línea de reporte en cada caso, acorde con el tema del cual son responsables.
	Comité Institucional de Gestión y Desempeño.	• Realizar seguimiento y análisis periódico a los riesgos institucionales y proponer mejoras a su estructura.
Primera Línea	Responsables de los Proceso Facilitadores para el SIG en los procesos	• Identificar y valorar los riesgos que pueden afectar el proceso, los programas, proyectos, planes y procedimientos a su cargo y actualizarlo cuando se requiera. • Definir, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados alineados con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso. • Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. • Desarrollar ejercicios de autoevaluación para establecer le eficiencia, eficacia y efectividad de los controles. • Informar a la Oficina Asesora de Planeación y Prospectiva o quien haga sus veces (segunda línea de defensa) sobre los riesgos materializados en los procesos, programas, proyectos y planes a su cargo. • Reportar al Comité Institucional de Gestión y

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
		Desempeño, los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado (cuando se requiera). • Presentar las acciones correctivas, preventivas y de mejora, cuando se materializa los riesgos, de acuerdo con el procedimiento "Procedimiento acciones preventivas, correctivas y de mejora (PR-SIG-06)"
Segunda Línea	Oficina Asesora de Planeación	• Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo.
	Administrador del SIG	• Consolidar el mapa de riesgos institucional (riesgos de mayor criticidad frente al logro de los objetivos) y presentarlo para análisis y seguimiento ante el Comité de Gestión y Desempeño Institucional. • Publicar los mapas de riesgos en la WEB • Presentar al Comité Institucional de Gestión y Desempeño, el seguimiento a la eficacia de los controles a los riesgos de los procesos. • Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración del riesgo. • Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los responsables de procesos. • Supervisar en coordinación con los demás responsables de esta segunda línea de defensa que la primera línea identifique, evalué y gestione los riesgos y controles para generar las acciones pertinentes. • Asesorar la identificación de los riegos institucionales, de corrupción y de seguridad de la información. • Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos.
	Oficial de Seguridad de la información	• Asesorar a los líderes de proceso en la identificación de los riegos de seguridad de la información. • Presentar al Comité Institucional de Gestión y Desempeño, el seguimiento a la eficacia de los

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
		controles a los riesgos de seguridad de la información de los procesos. • Asesorar a los líderes de los procesos en la implementación de los controles definidos
Tercera Línea	Jefe Oficina Asesora de Control Interno	• Asesorar de forma coordinada con la Oficina Asesora de Planeación y Prospectiva, a la primera línea de defensa en la identificación de los riesgos institucionales, de corrupción y de seguridad de la información y diseño de controles. • Llevar a cabo la evaluación independiente a los riesgos registrados en los mapas de riesgos de conformidad con el Plan Anual de Auditoría y reportar los resultados al Comité Institucional Coordinador de Control Interno - CICCI. • Recomendar a la línea estratégica mejoras a la política de administración del riesgo.

5.2 Comunicación y Socialización de la Política de Gestión del Riesgo

La política de administración del riesgo en el Ministerio de Agricultura y Desarrollo Rural será comunicada a todos los niveles de la organización, mediante alguno de los siguientes canales:

- Página WEB de la Entidad
- Camponet
- Correos electrónicos
- Procesos de Formación y Capacitación
- Ejercicios de Inducción y Re-Inducción

A través de estos canales se comunica o socializa contenidos relacionados con la gestión de los riesgos y aquellos orientados a generar conocimiento en los funcionarios y contratistas de la entidad.

5.3 Seguimiento al cumplimiento de la política, monitoreo y revisión de los riesgos

La aplicación de la Política de Administración del Riesgo es responsabilidad de todos los funcionarios y contratistas del Ministerio de Agricultura y Desarrollo Rural, la cual puede ser revisada por parte de la Línea Estratégica en cualquier momento, de acuerdo con las directrices que establezca el Comité Institucional de Coordinación de Control Interno. Las acciones que de esta revisión surjan deben ser adoptadas e implementadas por los responsables, de acuerdo con su nivel de responsabilidad (descrito en el numeral 5.1).

Se complementa su seguimiento a través de las siguientes disposiciones para el monitoreo y revisión de los riesgos:

- 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. Debe incluir en su revisión los riesgos institucionales, de corrupción y

Seguridad de la información; evaluando el diseño e idoneidad de los controles y demás aspectos indefinidos en las guías que el Departamento Administrativo de la Función Pública defina, comunicando a los responsables de los resultados del seguimiento y la evaluación realizados, así como los aspectos a mejorar.

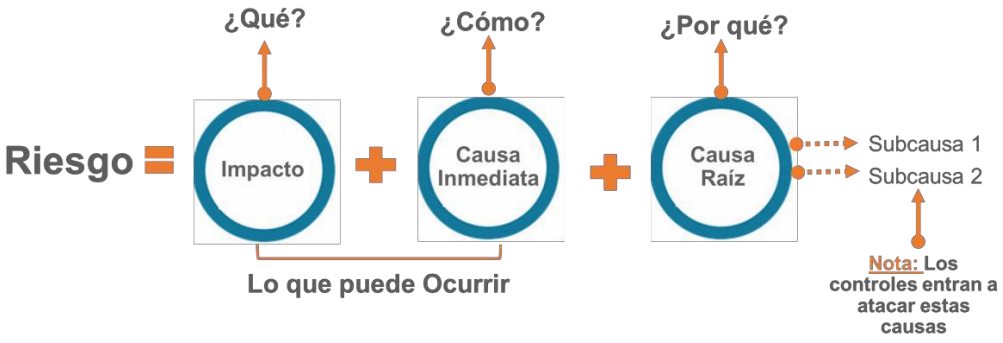
- Los responsables de procesos deberán como mínimo realizar un ejercicio de actualización del mapa de riesgos por lo menos una vez al año, verificando el cumplimiento de las directrices de esta política y las guías que al respecto expida el Departamento Administrativo de la Función Pública. Esta actualización tendrá el acompañamiento del Grupo Administración del SIG.
- Los responsables de procesos (Primeria línea de defensa) y sus equipos de trabajo deberán como mínimo en cada vigencia, realizar un seguimiento interno a los riesgos identificados, orientados a realizar el seguimiento, monitoreo y comportamiento sobre la aplicación de los controles, la definición de estos y su pertinencia; aplicando y sugiriendo los correctivos o ajustes necesarios para asegurar un efectivo manejo del riesgo.
- Para el establecimiento de los riesgos de seguridad de la información se deben tener en cuenta los activos de información identificados en cada proceso, donde se pueden identificar tres (3) tipos de riesgos: pérdida de confidencialidad, de la integridad y de la disponibilidad de los activos de información. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.
- Para el riesgo identificado se deben asociar el grupo de activos de información o activos de información específicos del proceso y conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.
- Se deben generar y registrar las acciones preventivas y correctivas resultado del ejercicio de seguimiento efectuado, de acuerdo con lo establecido en el “Procedimiento Acciones Preventivas, Correctivas y de Mejora (PR-SIG-06)”

5.4 Identificación de Riesgos

El Ministerio de Agricultura y Desarrollo Rural identifica los riesgos basados en el contexto organizacional, objetivos estratégicos, los objetivos y alcance de los procesos del SIG registrados en la caracterización de los procesos; analizando los factores internos y externos que afectan el cumplimiento de los objetivos institucionales.

Su redacción será la establecida en la guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas Versión 5:

Redacción de los riesgos de Gestión y de Seguridad de la Información (Digital)



Ejemplo: Posibilidad de incurrir en pérdidas económicas por multa o sanción del ente regulador debido a transmitir tarde el balance

Redacción de los Riesgos de Corrupción

Ejemplo: Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.

Los riesgos identificados se pueden clasificar de acuerdo con el siguiente criterio:

CLASIFICACIÓN DEL RIESGO	DESCRIPCION
Corrupción	Es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. Se establecen sobre el proceso.
Daños Activos Físicos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.
Ejecución y Administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fallas Tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Fraude Externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude Interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Relaciones Laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas, organizacionales	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.

5.5 Valoración del Riesgo

En la valoración del Riesgo se establece la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, para establecer la zona de riesgo inicial, es decir, el riesgo inherente; analizando y evaluando los riesgos a través de los controles establecidos, para finalmente establecer la zona de riego final, es decir, la zona residual; teniendo en cuenta los lineamientos establecidos en la mencionada guía de la función pública.

Determinación de la probabilidad.

La probabilidad se determinará de acuerdo con el número de veces que se pasa por el punto de riesgo en un periodo de un año, según el siguiente criterio:

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Determinación del impacto.

El impacto se determina de acuerdo con la afectación que puede tener el riesgo, el cual puede ser económico, reputacional o por impactos dados por corrupción; aplicando los criterios definidos en la siguiente tabla:

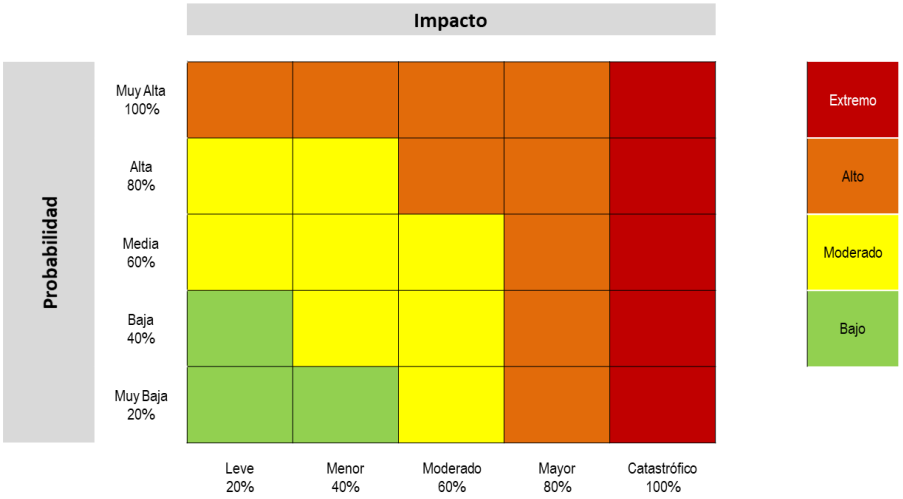
IMPACTO		AFECTACION DEL IMPACTO		
		ECONÓMICA	REPUTACIONAL	CORRUPCIÓN
Leve	20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de alguna área de la organización	
Menor	40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores	
Moderado	60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	La evaluación tiene de 1 a 5 criterios afirmativos
Mayor	80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal	La evaluación tiene de 6 a 11 criterios afirmativos
Catastrófico	100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país	La evaluación tiene de 12 a 19 criterios afirmativos

Para los riesgos de corrupción se analizarán únicamente para los siguientes niveles i) moderado, ii) mayor, y iii) catastrófico, dado que estos riesgos siempre serán significativos, en tal sentido, no aplican los niveles de impacto insignificante y menor, que sí aplican para las demás tipologías de riesgos. Para seleccionar el criterio que le aplica mostrados en la tabla anterior, se aplican los criterios mostrados a continuación:

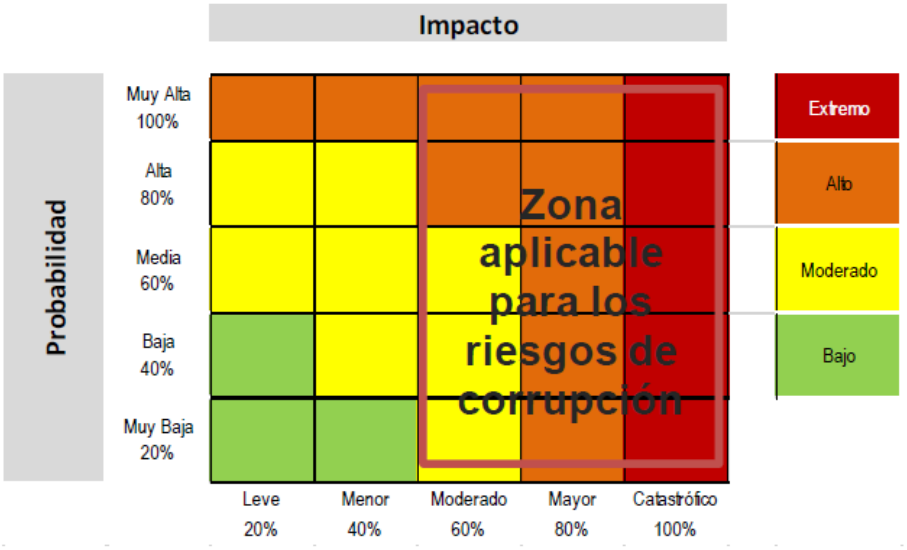
No.	PREGUNTA: SI EL RIESGO DE CORRPCIÓN SE MATERIALIZA PODRÍA …	RESPUESTA	
		SI	NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del 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.			

No.	PREGUNTA: SI EL RIESGO DE CORRPCIÓN SE MATERIALIZA PODRÍA …	RESPUESTA SI	RESPUESTA NO
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.		

Para determinar los niveles de severidad de los riesgos a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor, teniendo en cuenta el siguiente gráfico:



Analizado la probabilidad y el Impacto para los Riesgos de Corrupción aplicando controles, se obtiene matriz de calor para riesgos de corrupción de acuerdo con el siguiente cuadro:



5.6 Identificación del control y valoración del riesgo residual

Los controles una vez se identifiquen deben ser coherentes y estar dirigidos a minimizar las causas inmediatas y su redacción se realiza de acuerdo con lo establecido en el numeral 3..2.2.1 de la guía de administración del riesgo y diseño de controles para entidades públicas.

Para el análisis y valoración de los controles, teniendo en cuenta las características relacionadas con la eficiencia y la formalización, se realiza de acuerdo con la siguiente tabla:

Características			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	15%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	25%
Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	
		Sin Documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	
		Sin registro	El control no deja registro de la ejecución del control.	

Nota: Esta evaluación es realizada en el formato de Mapa de Riesgo establecida por el Ministerio de Agricultura y Desarrollo Rural.

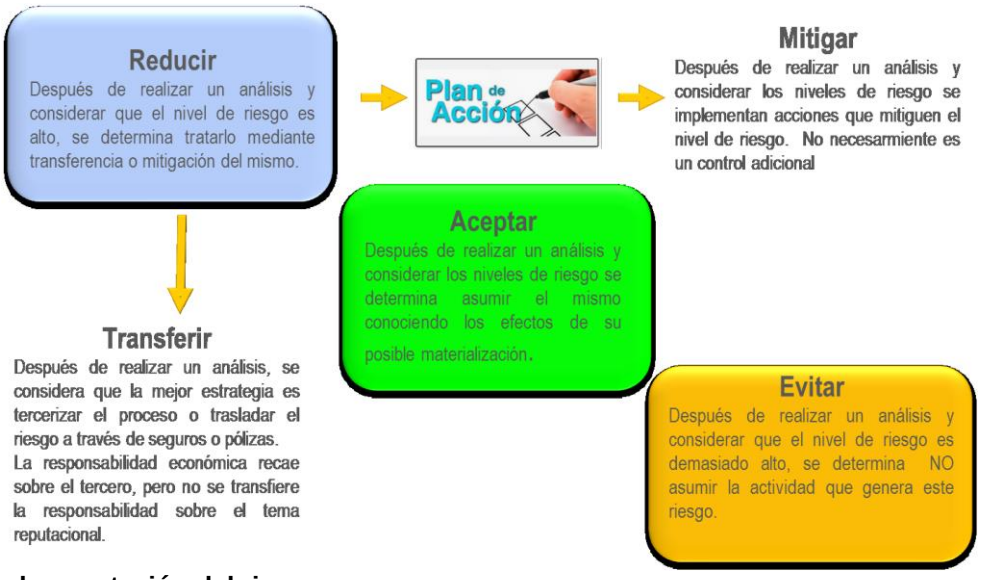
Para la aplicación de los controles se debe tener en cuenta que estos mitigan el riesgo de forma acumulativa, es decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control, y de esta forma se calcula el riesgo residual.

Los controles preventivos y detectivos reducen en el riesgo residual la probabilidad; y los correctivos el impacto.

Para los controles que no están implementados, se establece un plan de tratamiento de riesgos. Para los riesgos de seguridad de la información, la Oficina de Tics coordinará con los responsables la implementación de los controles definidos y el respectivo plan de tratamiento de riesgos; quien además le hará seguimiento a las actividades y compromisos definidos en el marco del plan de tratamiento de riesgos, llevando un registro en los mecanismos o herramientas que para tal fin implemente.

Estrategias para combatir el riesgo

El Ministerio de Agricultura y Desarrollo Rural, establece que el nivel de riesgo en aceptar, reducir o evitar. Se analiza frente al riesgo residual, esto para procesos en operación, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente. En el siguiente cuadro se identifican las opciones para combatir el riesgo teniendo en cuenta el Plan de Acción a que allá lugar:

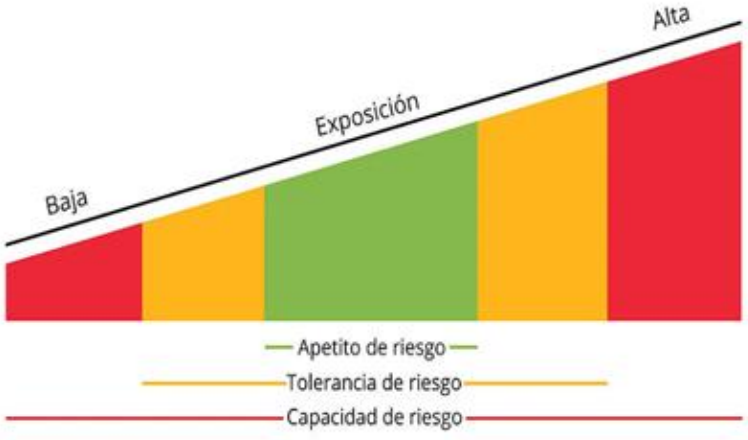


5.7 Niveles de aceptación del riesgo

Los niveles del riesgo para el Ministerio de Agricultura y Desarrollo Rural, son definidos a partir del valor resultante de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. Así mismo,

de los resultados obtenidos se establece los valores admisibles para el Ministerio y para ello se deben establecer los siguientes niveles para la entidad y sus valores, así:

NIVELES DE ACEPTACIÓN	DEFINICIÓN	VALORES ADMISIBLES SEGÚN TIPO DE RIESGOS		
		Riesgos de Gestión	Riesgos de Corrupción	Riesgos de Seguridad de la Información
Apetito del riesgo	Es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.	Bajo, Moderado	Bajo	Bajo
Tolerancia del riesgo	Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.	Moderado	N/A	Moderado
Capacidad del riesgo	Es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad	Alto	Alto	Moderado

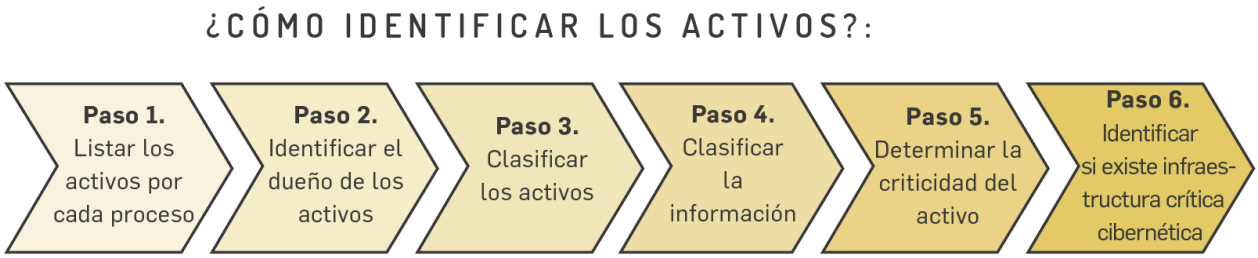


Los valores de los niveles de aceptación de riesgos son tomados a partir de los riesgos residuales y cuando los riesgos superen la capacidad del riesgo, la alta dirección los acepta siempre que se tengan controles establecidos que afecten positivamente al cumplimiento de los objetivos y que el responsable del proceso garantice su aplicación de forma estricta, se deben establecer acciones preventivas o planes de tratamiento de riesgos para evitar su materialización o mejorar el fortalecimiento del control.

Así mismo los riesgos que su valoración residual coinciden con la Capacidad de riesgo, los lideres de los procesos deben hacer una verificación dentro de la vigencia donde se revise que estos se están realizando de acuerdo a lo definido y de encontrar desviaciones iniciar las acciones correctivas que correspondan.

5.8 Riesgos de seguridad de la información

Para la identificación de los riesgos de Seguridad de la Información, se debe tener en cuenta la Política de Seguridad y Privacidad de la Información (DE-GGT-03), del Ministerio Agricultura y Desarrollo Rural, que propende por preservar las características de confidencialidad, integridad y disponibilidad de los activos de información que hacen parte de cada uno de los procesos institucionales, para lo cual es fundamental identificar y valorar los activos de información institucionales. Estos activos se identifican teniendo en cuenta los siguientes pasos:



Para la valoración de riesgos inherentes de la seguridad de los diferentes activos de información identificados se requiere que sus propietarios identifiquen, dentro del contexto interno y externo de la entidad, las consecuencias que tendría la pérdida de su confidencialidad, integridad o disponibilidad, en el peor caso posible, es decir sin tener en cuenta medidas de seguridad existentes en el Ministerio, por lo tanto, se debe tener en cuenta la perdida de:

- Confidencialidad
- Integridad
- Disponibilidad

Los activos de información se clasifican en:

- Físico
- Información
- Personal
- Procesos
- Red
- Servicios
- Software

La valoración de los activos de información se realiza en una escala de 1 a 5, teniendo en cuenta los siguientes criterios:

Valoración CID	Descripción
1	Daño insignificante
2	Daño menor
3	Daño considerable
4	Daño grave
5	El cumplimiento de la misionalidad institucional se ve amenazada por la pérdida de la confidencialidad, integridad o disponibilidad del activo de

	información

Para la valoración de los activos de información se tiene en cuenta la siguiente tabla:

Una vez identificados y valorados los activos de información de cada uno de los procesos, se analizan las amenazas que pueden explotar vulnerabilidades existentes en estos, evaluándolas de 0 a 3, de acuerdo con la siguiente tabla:

Nivel de Amenaza	Descripción	Justificación
0	La amenaza no está presente en el entorno del activo dentro del contexto de la organización.	Requiere
1	La amenaza se considera presente en el entorno del activo dentro del contexto de la entidad y con baja probabilidad de que explote vulnerabilidades dentro del alcance.	Requiere
2	La amenaza se considera presente en el entorno del activo dentro del contexto de la entidad y con media probabilidad de que explote vulnerabilidades dentro del alcance.	No requiere
3	La amenaza se considera presente en el entorno del activo dentro del contexto de la entidad y con alta probabilidad de que explote vulnerabilidades dentro del alcance.	No requiere

Del mismo modo se realiza la evaluación de vulnerabilidades de los diferentes activos de información, para lo cual se tiene en cuenta la siguiente tabla:

Vulnerabilidad	Descripción	Justificación
0	La vulnerabilidad no aplica al activo dentro del contexto de la entidad, por lo que el control no se aplica.	Requiere
1	Es muy improbable que la vulnerabilidad sea explotada, ya que el control está implantado de forma eficiente y ha sido auditado sin registrarse incumplimientos.	Requiere
2	Es poco probable que la vulnerabilidad sea explotada en el futuro, ya que el control está implantado de forma eficiente.	Requiere
3	Es probable que la vulnerabilidad sea explotada en el futuro, ya que el control se ha implantado parcialmente o de forma deficiente.	Requiere
4	Es muy probable que la vulnerabilidad sea explotada en el futuro ya que el control no se ha implantado.	No requiere

5	La vulnerabilidad ha sido explotada en el pasado, más allá del nivel de implantación del control.	No requiere

A partir de la valoración de confidencialidad, disponibilidad e integridad de los diferentes activos de información y el análisis de amenazas y vulnerabilidades, se obtiene el nivel de riesgos, así:

$$R_a = I_a * Max(A_a * V)$$

R_a: Riesgo sobre el activo.

I_a: Impacto sobre el activo en términos de confidencialidad, integridad y disponibilidad.

A_a: Amenaza en el entorno sobre el activo.

V: Vulnerabilidad.

A continuación, se presenta el mapa de calor de gestión de riesgos de seguridad de la información:

	Nivel de Amenaza	1					2					3				
	Nivel de Vulnerabilidad	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Valor del Activo	1	1	2	3	4	5	2	4	6	8	10	3	6	9	12	15
	2	2	4	6	8	10	4	8	12	16	20	6	12	18	24	30
	3	3	6	9	12	15	6	12	18	24	30	9	18	27	36	45
	4	4	8	12	16	20	8	16	24	32	40	12	24	36	48	60
	5	5	10	15	20	25	10	20	30	40	50	15	30	45	60	75
		Nivel de Riesgo														

Los datos reflejados en la tabla anterior se interpretarán de la siguiente manera:

Nivel de Riesgo	Descripción
1 – 24 Bajo	No es necesario adoptar ninguna medida. El nivel de riesgo es suficientemente bajo y no justifica la implantación de controles adicionales.
25 – 48 Moderado	La dirección de la empresa, o un delegado de esta, determinará el nivel de los riesgos que son aceptables o no a su juicio. El Responsable de Seguridad que gestiona el SGSI determinará los controles que tendrán que aplicarse para mitigar los riesgos.
49 – 75 Alto	El nivel de riesgos no es aceptable, y sólo se podrán excluir controles que los mitiguen justificando dicha exclusión por parte de la dirección de la empresa. El Responsable de Seguridad que gestiona el SGSI determinará los controles que tendrán que aplicarse para mitigar los riesgos.

La gestión del riesgo se realiza a través de cuatro estrategias, las cuales son:

- Aceptar.
- Tratar.
- Transferir.
- Evitar.

Aceptar el riesgo

La Entidad puede aceptar riesgos que no tratará de ninguna manera en los casos que:

- El riesgo sea menor o igual al nivel de riesgo aceptable.
- El costo de tratar el riesgo sea mayor que el daño que pueda causar su impacto.
- El costo de tratar el riesgo no pueda ser asumido económicamente. En este caso deberán considerarse opciones adecuadas al presupuesto para el tratamiento, aunque no sean las idóneas.

Para cualquiera de estas situaciones, se justificará debidamente las razones por las que el riesgo se acepta.

Tratar el riesgo

La Entidad decidirá, la prioridad en la implantación de las medidas de tratamiento de riesgo, en proporción al nivel de riesgo, la facilidad de la implantación, el costo o a los cambios en la entidad.

1. Riesgo ALTO: Si el nivel de riesgo resultante para un activo es igual o superior a 49, a partir de la norma ISO/IEC 27001:2013 Anexo A se seleccionarán los objetivos de control y controles que mitiguen el riesgo a un nivel aceptable y que encajen con los requisitos establecidos por la Entidad. En relación con los activos y a sus vulnerabilidades/amenazas asociadas, se implantarán todos los controles adicionales que tengan un efecto positivo en la misionalidad institucional y en los procesos existentes y cuyo costo sea aceptable.

2. Riesgo MODERADO: Se puede aceptar un riesgo con un nivel entre 25 y 49 por cualquiera de las razones expuestas a continuación:

    a) El control o el proceso asociado no está alineado con la cultura de la organización.
    b) El personal necesario para su operación no está disponible.
    c) Los recursos económicos necesarios no están disponibles.
    d) No existe un beneficio claro para la Entidad.
    e) El coste de implantación del control supera el coste del activo que protege o el coste de una brecha de seguridad actual o futura.

La aceptación del riesgo debe quedar documentada. En caso de no aceptación del riesgo, se actuará, como se indica para el caso de riesgo ALTO, seleccionando los procedimientos, mejores prácticas y mecanismos que mitiguen el riesgo a un nivel aceptable.

3. Riesgo BAJO: Los niveles de riesgo entre 1 y 24 son bajos y no requieren actuación ninguna.

Se determina que un riesgo ALTO es inaceptable para la Entidad, a menos que así lo decida la línea de defensa estratégica y sobre el que dependa la propiedad y el derecho de uso del activo afectado mediante la justificación de dicha decisión.

Transferir el riesgo

Cuando sea conveniente, la entidad podrá transferir el riesgo a otras entidades. En caso de optar por transferir un riesgo, las acciones tomadas deben quedar documentadas y ser revisadas. Las responsabilidades transferidas se reflejarán en acuerdos de nivel de servicio.

Se registrarán las actuaciones llevadas adelante en la transferencia de los riesgos.

Evitar el riesgo

La Entidad también puede optar por evitar el riesgo cesando un proceso o actividad o modificando la forma en que este se lleva a cabo. En caso de optar por evitar un riesgo, las acciones tomadas deben quedar documentadas y ser revisadas.

Si el proceso o actividad son modificados, deberá realizarse el análisis de riesgos para el proceso o actividad modificada, no así en caso de cese de este.

Se registrarán las actuaciones llevadas adelante para evitar los riesgos.

Aceptación del riesgo residual

El riesgo residual para cualquiera de los activos y una vez aplicados las medidas de control previstas deberían situarse en un rango de valores por debajo del valor de riesgo aceptable determinado por la Entidad.

Para aquellos casos en que, tras el tratamiento con los controles previstos, se determine un nivel de riesgo moderado, se deberá obtener la aprobación de la línea de defensa estratégica para aceptar el riesgo residual resultante, lo cual deberá ser documentado.

Vulnerabilidad Residual	Descripción
0	La vulnerabilidad residual no aplica al activo porque la amenaza no aplica, o porque el conjunto de controles no aplica.
1	Es muy improbable que la vulnerabilidad residual sea explotada, ya que el conjunto de controles estará implantado y auditado.
2	Es poco probable que la vulnerabilidad residual sea explotada en el futuro, ya que el conjunto de controles estará implantado.
3	La vulnerabilidad residual es parcial ya que el activo ha sido evaluado metodológicamente y se ha decidido aceptar su riesgo.

Realizada la gestión de riesgos, se obtiene la Declaratoria de Aplicabilidad y el Plan de Tratamiento de Riesgos.

De conformidad con la Política de Seguridad y Privacidad de la Información (DE-GGT-03), del Ministerio Agricultura y Desarrollo Rural, lo anterior se realiza a través del aplicativo establecido por la Oficina de TICs, quien coordina todo el proceso de identificación de los activos de información con los responsables

de los procesos y establece las valoraciones con los mismos. Así mismo establece los planes de gestión de riesgos a los cuales tenga lugar y realiza los seguimientos a los mismos.

La información del aplicativo se traslada al formato “Mapa de Riesgos (F01-PR-SIG-05)” y se publica en la página WEB, de acuerdo con las orientaciones del Grupo Administración del SIG

5.9 Acciones ante los riesgos materializados

Cuando se materializan riesgos identificados en la matriz de riesgos institucionales se deben aplicar las acciones descritas en la siguiente tabla:

Tipo de Riesgo	Responsable	Acción
Riesgo de Corrupción	Líder de Proceso	Informar al Oficina Asesora de Planeación y Prospectiva y Grupo de Administración del Sistema Integrado de Gestión (como segunda línea de defensa en el tema de riesgos) sobre el posible hecho encontrado. Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), contribuir para determinar la aplicabilidad del proceso disciplinario. Identificar las acciones correctivas necesarias y documentarlas en el plan de mejoramiento. Efectuar el análisis de causas y determinar acciones preventivas y de mejora. Revisar los controles existentes y actualizar el mapa de riesgos.
	Oficina de Control Interno	Informar al líder del proceso y a la segunda línea de defensa, quienes analizarán la situación y definirán las acciones a que haya lugar. Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), determinar la aplicabilidad del proceso disciplinario. Informar a discreción los posibles actos de corrupción al ente de control.
Riesgos de Gestión y Seguridad digital	Líder de Proceso	Informar al Oficina Asesora de Planeación y Prospectiva y Grupo de Administración del Sistema Integrado de Gestión como segunda línea de defensa, el evento o materialización de un riesgo. Proceder de manera inmediata a aplicar el plan de contingencia o de tratamiento de incidentes de seguridad de la información que permita la continuidad del servicio o el restablecimiento de este (si es el caso) y documentar en el plan de mejoramiento.

Tipo de Riesgo	Responsable	Acción
		Realizar los correctivos necesarios frente al cliente e iniciar el análisis de causas y determinar acciones correctivas, preventivas, y de mejora, así como la revisión de los controles existente, documentar en el plan de mejoramiento institucional y actualizar el mapa de riesgos. Dar cumplimiento al procedimiento plan de mejoramiento.
	Oficina de Control Interno	Informar al líder del proceso sobre el hecho encontrado Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos. Verificar que se tomen las acciones y se actualice el mapa de riesgos correspondiente. Si la materialización de los riesgos es el resultado de una auditoría realizada por la Oficina de Control Interno, esta verificará el cumplimiento del plan de mejoramiento y realizará el seguimiento de acuerdo con el procedimiento.

5.10 Otras disposiciones con relación a la gestión de los riesgos

- Para cada riesgo de seguridad de la información, se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. El Ministerio de Agricultura y Desarrollo Rural acoge las tablas establecidas en el Anexo 4 del Modelo Nacional de Gestión de Riesgos de Seguridad de la información para entidades públicas.

- 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.

- 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 de seguridad de la información en coordinación con el Grupo Administración del SIG.

- 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 riesgos 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, de seguridad de la información y los de corrupción, por separado y de forma consolidada para conocimiento y consulta de la ciudadanía.

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”.

Fecha	Versión	Descripción
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
06-05-2021	11	Se ajustó la estructura 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 Púbica – Versión 5 del 2020. Su contenido se aprobó en sesión del Comité Institucional Coordinador de Control Interno, el día 06 de mayo de 2021.
27-05-2022	12	Se ajustó el glosario, las condiciones, seguimiento al cumplimiento de la política, monitoreo y revisión de los riesgos, Identificación de Riesgos e inclusión de Acciones ante los riesgos materializados. Su contenido se aprobó en sesión del Comité Institucional Coordinador de Control Interno, el día 27 de mayo de 2022