MINAGRICULTURA	PROCEDIMIENTO	VERSIÓN 12
	Gestión del Riesgo	PR-SIG-05
		FECHA EDICIÓN 17-05-2016

1. OBJETIVO

Determinar los lineamientos que deben ser aplicados por el Ministerio de Agricultura y Desarrollo Rural, para el desarrollo e implementación de la Política de Administración del Riesgo con el fin de evitar obstáculos en el cumplimiento de la misión y el logro de los objetivos institucionales.

2. ALCANCE

Desde la identificación de los riesgos asociados a los procesos y productos del Ministerio, su análisis, valoración y la identificación de controles preventivos o correctivos, hasta la implementación de acciones de manejo y seguimiento respectivo.

3. BASE LEGAL

- Ley 87 de 1993
- Ley 1474 de 2011 articulo 73
- Decreto 1537 de 2001
- Decreto 2641 de 2012
- Decreto 943 de 2014
- Decreto 2573 de 2014

4. DEFINICIONES

1. **ADMINISTRACIÓN DEL RIESGO:** Conjunto de elementos que le permiten a la entidad autocontrolar aquellos eventos que puedan afectar el cumplimiento de sus objetivos

2. **ANÁLISIS DE RIESGO:** Permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad para su aceptación y manejo.

3. **CAUSAS DEL RIESGO:** Factores internos o externos (medios, circunstancias y agentes), sujetos u objetos (personas, materiales, comités, instalaciones, entorno) capaces de originar el riesgo.

4. **CONTROL DEL RIESGO:** Toda acción que tiende a minimizar los riesgos. Significa analizar el desempeño de las operaciones evidenciando posibles desviaciones frente al resultado esperado, para la adopción de medidas preventivas.

5. **DESCRIPCIÓN DEL RIESGO:** Característica general o la forma en que se observa o pudiera manifestar el riesgo identificado

6. **EFECTOS DEL RIESGO:** Consecuencia que puede ocasionar a la entidad la materialización del riesgo (daños físicos, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental).

7. **IMPACTO DEL RIESGO:** Valoración anticipada de la gravedad del daño cuando eventualmente se materializa un riesgo.

REVISO	APROBO
HERACLIO BEJARANO CRUZ COORDINADOR GRUPO ADMINISTRACION DEL SIG FECHA: 17-05-2016	ALEJANDRA PAEZ OSORIO SECRETARIA GENERAL FECHA: 17-05-2016

8. **MADR:** Ministerio de Agricultura y Desarrollo Rural.

9. **MAPA DE RIESGOS:** Herramienta metodológica que permite hacer un inventario de los riesgos ordenada y sistemáticamente, definiéndolos, haciendo la descripción de cada uno de estos y las posibles consecuencias.

10. **PROBABILIDAD DEL RIESGO:** Medida para estimar la posibilidad de que ocurra o pueda presentarse el riesgo.

11. **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 y consecuencia.

12. **RIESGO RESIDUAL:** Nivel de riesgo que permanece luego de aplicar controles que eviten la materialización de los riesgos inicialmente identificados.

13. **PLANES DE CONTINGENCIA:** Documento que contiene las acciones alternas a ejecutar en caso de la materialización del riesgo, con el fin de permitir la continuidad a los procesos de la entidad.

14. **TICs**: Tecnologías de la Información y las Comunicaciones

5. CONDICIONES GENERALES

1. El contexto estratégico es revisado por el Grupo de Administración del SIG, en coordinación con los responsables de los procesos, basándose en las actividades definidas en el "hacer" de la respectiva caracterización, identificando aquellos factores internos o externos que pueden afectar el cumplimiento de los objetivos del proceso y posteriormente se resumen en el informe de gestión del riesgos.

2. Para los riesgos "tecnológicos" y "seguridad de la información" identificados en los procesos, la Oficina de TICs es la responsable de realizar el acompañamiento en su identificación, análisis y valoración, así mismo en identificar los controles necesarios.

3. Los controles para el tratamiento de los riesgos "Seguridad de la información" son seleccionados por la Oficina de TICs de acuerdo a los parámetros definidos en la Norma Técnica NTC ISO 27001, especialmente aquellos controles recomendados en el Anexo A de la misma.

4. Para los riesgos "Seguridad de la información" identificados, los controles que se establezcan deben ser documentados en el formato "declaración de aplicabilidad de controles de seguridad de la información (F02-PR-SIG-05)", por la Oficina de TICs, e identificar el estado dentro de la entidad, los cuales pueden ser: seleccionado, implementado o excluido.

5. Para los riesgos "Seguridad de la información" que estén en estado seleccionado, el responsable del proceso y la Oficina TICs deben adelantar las actividades necesarias para implementarlo y se considera como una fase en el proceso de establecimiento de los riesgos, como lo define el numeral 4.1 numeral g, de la norma NTC GP:1000.

6. DESARROLLO

Nº	ACTIVIDAD	RESPONSABLE	DOCUMENTO
1	Identificar, analizar y valorar los riesgos a los cuales está expuesto el proceso y/o producto del MADR, aplicando los criterios definidos en el anexo 1 de este procedimiento.	Dueño de proceso o responsable de la actividad definido en la caracterización del proceso	
2	Elaborar el mapa de riesgos del Proceso registrando la información concluida en la etapa anterior, en el formato "F01-PR-SIG-05 Mapa de Riesgos".	Dueño de proceso o responsable de la actividad definido en la caracterización del proceso	F01-PR-SIG-05 Formato Mapa de Riesgos
3	Verificar los riesgos definidos, si cumplen requisitos generales, imprime y pase para firmas. Nota 1: para los riesgos de corrupción de manera previa se debe efectuar una consulta tanto interna como externa a través de alguno de los canales de comunicación definidos dentro de la entidad antes de pasar a firmas. Nota 2: para los riesgos de "seguridad de la información" serán verificados por la Oficina de TICs, de acuerdo a lo establecido en el numeral 2 y 3 de las condiciones generales de este procedimiento.	Coordinador Grupo Administración del SIG Profesional asignado por la Oficina de TICs	F01-PR-SIG-05 Formato Mapa de Riesgos
4	Aprobar el mapa de riesgos del proceso	Dueño de proceso o responsable de la actividad definido en la caracterización del proceso	F01-PR-SIG-05 Formato Mapa de Riesgos
3	Realizar la divulgación del Mapa de Riesgo a los integrantes del proceso.	Dueño de proceso o responsable de la actividad definido en la caracterización del proceso	Registro de divulgación (email, memorando o formato F03-PR-SIG-02 difusión de documentos"
4	Elaborar el mapa de riesgos institucional.	Coordinador Grupo Administración del SIG	F01-PR-SIG-05 Formato Mapa de Riesgos
5	Realizar el seguimiento permanente al comportamiento de los riesgos y a la aplicación de los controles establecidos para mitigarlos. © Nota 1: Si detecta no conformidades o posibilidades de mejora, genere acciones correctivas, preventivas o de mejora, de acuerdo al procedimiento "PR-SIG-06 Acciones Preventivas, Correctivas y de Mejora".	Dueño de proceso o responsable de la actividad definido en la caracterización del proceso	F01-PR-SIG-06 Formato Solicitud Acciones Preventivas, Correctivas o de Mejora
6	Realizar la verificación de aplicación de los controles existentes y determine si estos son	Coordinador Grupo Administración del SIG	Informe Gestión del Riesgo

N°	ACTIVIDAD	RESPONSABLE	DOCUMENTO
	efectivos para minimizar el riesgo. © Nota: Para los riesgos "tecnológicos" y "seguridad de la información", la verificación de la efectividad de controles es realizada por la Oficina de TICs.	Profesional asignado por la Oficina de TICs	
7	Elabore el informe de gestión del riesgo del Ministerio.	Coordinador Grupo Administración del SIG	Informe Gestión del Riesgo
8	Realice seguimiento y evaluación a la gestión de riesgos de los procesos. ©	Jefe de la Oficina de Control Interno	
9	Presente informe de los resultados del seguimiento y evaluación con recomendaciones de mejoramiento y tratamiento a las situaciones detectadas.	Jefe de la Oficina de Control Interno	Informe Oficina de Control Interno, formato para solicitud de acciones preventivas, correctivas o de mejora (F01-PR-SIG-06)

7. DOCUMENTOS DE REFERENCIA

- DE-DEI-05 Política de Administración del Riesgo
- Guía de Administración del Riesgo, DAFP.
- Estrategias para la construcción del Plan Anticorrupción y de Atención al Ciudadano, presidencia de la república – secretaria de transparencia
- Manual de Implementación Modelo de Control Interno para Entidades del Estado
- F01-PR-SIG-05 Formato Mapa de Riesgos
- F02-PR-SIG-05 Declaración de aplicabilidad de controles de seguridad de la información
- F01-PR-SIG-06 Formato para solicitud de acciones preventivas, correctivas o de mejora
- NTC ISO 27001: 2013 Sistemas de Gestión de la Seguridad de la Información

8. HISTORIAL DE CAMBIOS

Fecha	Versión	Descripción
25-09-2008	2	Se cambió en el alcance plan de manejo por acciones de manejo. Se eliminó en las definiciones plan de manejo de riesgos. Se modificaron, en las condiciones generales, los criterios, que se deben aplicar en la evaluación del riesgo. En el cuadro de desarrollo, se eliminó la actividad No. 20.
19 -05-2009	3	Se incluyeron las definiciones de planes de contingencia e indicadores. En las condiciones generales del procedimiento se colocó la nota de la elaboración de los planes de contingencia cuando la calificación del impacto es catastrófico. Se incluyeron las actividades No. 18 y 20.
01-06-2009	4	Se incluyeron en las Condiciones Generales, las tablas de eficacia y eficiencia y la fórmula para medir la efectividad de los controles. Se eliminó la definición de indicadores. Se modificaron

Fecha	Versión	Descripción
		las actividades del cuadro de desarrollo. Se incluyó en los documentos de referencia la política de administración del riesgo, el Manual de implementación del Modelo de Control Interno para Entidades del Estado y el formato de difusión de documentos.
29-07-2009	5	Se incluyó la actividad 29 del cuadro de desarrollo.
03-02-2010	6	Se ajustó el objetivo, el alcance y la base legal. Se adicionaron definiciones. Se incluyeron en las condiciones generales ejemplos de los efectos más comunes que generan los riesgos y de distintos tipos de control. Igualmente se adicionaron las opciones de manejo del riesgo. Se ajustaron las actividades del cuadro de desarrollo.
02-09-2010	7	Se ajustó el cuadro de medición de la eficacia de los controles y se identificaron las actividades de control del cuadro de desarrollo.
26-04-2011	8	Se ajustó el alcance. Se incluyeron las actividades 1 y 2, y se reubicó la actividad 11. Se ajustaron los documentos de referencia.
29-05-2013	9	Se ajustó la base legal incluyendo la ley 1474 de 2011, se retiró del alcance la frase "y la medición de su efectividad", se ajustó las condiciones generales (sección 5) y el desarrollo (sección 6), se actualizo el logo del MADR de acuerdo a la nueva imagen y directrices del Manual de Identidad Institucional
31-03-2014	10	Se revisó el documento el contenido, se adicionó en la base legal el decreto 2641 de 2012.
16-04-2015	11	Se revisó y ajusto el documento en su contenido verificando el cumplimiento de las directrices establecidas para la "Política de Administración del Riesgo – DE-DEI-05", y se eliminó el numeral "5.1.5. Políticas de Administración de Riesgos".
17-05-2016	12	Se revisó: el objetivo, el alcance, numeral 5. "condiciones generales" y numeral 6 "desarrollo" en su contenido general. Se adicionó el anexo 1 para ampliar información sobre los criterios de evaluación de los riesgos, se incorporó el uso del formato F02-PR-SIG-05.

ANEXO 1
Criterios para el análisis y evaluación de los riesgos

La administración del riesgo en el MADR - Ministerio de Agricultura y Desarrollo Rural consta de cinco elementos de control: Contexto Estratégico, Identificación de Riesgos, Análisis de Riesgos, Valoración de Riesgos y Políticas de Administración de Riesgos. A continuación se definen los principales aspectos a tener en cuenta cuando se efectúe la revisión de cada uno de estos componentes:

a) Contexto Estratégico

Permite establecer los factores internos y externos (causas) que generan posibles situaciones de riesgo. El análisis se realiza a partir del conocimiento de situaciones del entorno de la entidad, teniendo en cuenta los aspectos de carácter social, económico, cultural, de orden público, político, legal y/o cambios tecnológicos, entre otros. También se tiene en cuenta el análisis de la situación de la entidad, basado en los resultados y cumplimiento de los planes y programas, la estructura organizacional, el modelo de operación, los sistemas de información, procesos y procedimientos y los recursos económicos, entre otros.

Para evaluar el contexto estratégico dentro de la entidad se debe verificar lo siguiente:

- **Factores externos**: cambios legales, constitucionales, jurisprudenciales, aspectos de orden público, aspectos culturales, aspectos sociales, reformas a la administración y recortes presupuestales.

- **Factores internos:** manejo de los recursos, la estructura organizacional, los controles existentes, los procesos y procedimientos, la disponibilidad presupuestal, la forma de vinculación del personal a la entidad, los intereses de los directivos, el nivel del talento humano, la motivación y los niveles salariales.

Para los riesgos de "**seguridad de la información**" por estar asociado a componentes tecnológicos, el contexto estratégico se puede precisar aplicando lo siguiente:

- Precise el proceso en donde se llevará a cabo el análisis de riesgos de seguridad de la información. Es importante contar con la mayor cantidad de información, determinando como mínimo: descripción del proceso, procedimientos, instructivos y/o cualquier otro documento que permita comprender el alcance y características del proceso y la identificación de los activos de información del MADR.

- Identifique los activos de información que hacen parte del proceso, teniendo como premisa que un activo de información se refiere a cualquier información o elemento relacionado con su tratamiento, que tenga valor para el MADR. Por lo anterior, se recomienda realizar una revisión de los activos de información críticos, como lo son los sistemas de información, *software*, *hardware*, documentos físicos y personas que permitan llevar a cabo el desarrollo normal del proceso.

  La identificación de los activos de información genera como resultado un inventario de activos de información, determinando al responsable del activo y los datos de identificación, así como los posibles riesgos de seguridad que puedan llegar a vulnerar la integridad, confidencialidad o disponibilidad de la información.

- Identifique las amenazas que podrían afectar los activos de información, entendiendo amenaza como el agente que puede explotar las vulnerabilidades de los activos afectando la seguridad de

la información. La identificación de las amenazas se puede llevar a cabo a través de la experiencia del Responsable del Activo o grupo de usuarios, o del conocimiento de los funcionarios de la entidad, entre otros medios. Otras fuentes son estándares internacionales para la gestión de riegos de seguridad de la información como Magerit o ISO27005.

Las amenazas pueden ser de origen natural o humano, ser accidentales o deliberadas. Una amenaza puede tener su origen dentro o fuera del MADR, un ejemplo de ellas podría ser; acciones no autorizadas, daño físico, fallas técnicas, entre otras. Sin embargo, para mayor claridad, en la siguiente tabla se relacionan algunos ejemplos:

Tipo de amenaza	**Amenazas**
Daños físicos	Fuego
	Daños por agua
	Polución
	Destrucción de equipo o medios de comunicación
	Polvo, Corrosión, Congelamiento
Eventos naturales	Fenómenos climáticos
	Fenómenos sísmicos
	Fenómenos volcánicos
	Inundación
Perdida de servicios esenciales	Falla en el suministro de agua o aire acondicionado
	Falla de suministro de energía
	Falla de equipos de telecomunicaciones
	Impulsos electromagnéticos
Perturbaciones por radiación	Radiación electromagnética
	Radiación térmica
	Impulsos electromagnéticos
Información comprometida	Interceptación de señal
	Espionaje remoto
	Hurto de medios o documentos
	Hurto de equipos
	Recuperación de medios reciclados o desechados
	Divulgación
	Datos provenientes de fuentes no confiables
	Manipulación de *hardware*
	Manipulación de *software*
Fallas técnicas	Falla de equipo
	Mal funcionamiento del equipo
	Saturación de sistema de información
	Mal funcionamiento del *software*
	Mantenimiento inadecuado del sistema
Acciones no autorizadas	Uso no autorizado del equipo
	Copia fraudulenta de *software* o de información
	Uso de *software* ilegal
	Corrupción de datos
	Procesamiento ilegal de datos
Compromiso de funciones	Error en el uso
	Abuso de derechos de acceso
	Falsificación de las credenciales de acceso
	Denegación de acciones
Humanas	Pirata informático, intruso ilegal
	Criminal informático

	Terrorismo
	Espionaje industrial
	Intrusos

Tabla 1. Ejemplos de posibles amenazas a los activos de información

- Identifique las vulnerabilidades o debilidades que pueden ser explotadas por las amenazas, su identificación se realiza por medio de pruebas técnicas como el análisis de vulnerabilidades con herramientas automáticas, inspección, observación, entre otras técnicas, que me permitan prever posibles situaciones que puedan poner en peligro la confidencialidad, integridad o disponibilidad del activo de información. En la Tabla relacionada a continuación se muestran algunos ejemplos de vulnerabilidades que se pueden tener presentes:

Tipo	Vulnerabilidad
Hardware	Falla o insuficiencia en los mantenimientos
	Falta de esquemas de reemplazo de equipos o piezas
	Susceptibilidad de polvo, humedad, barro
	Sensibilidad a la radiación electromagnética
	Falla o ausencia de suministro eléctrico
	Susceptibilidad a las variaciones de temperatura
	Bodegas sin protección
	Ausencia de procedimiento de destrucción y disposición final de medios
	Copias no controladas
Software	Ausencia de procesos de pruebas
	Fallas conocidas en el *software*
	No control de las sesiones de usuario
	Reutilización de medios de almacenamiento sin borrado seguro
	Ausencia de logs o trazabilidad de las actividades para auditoría
	Asignación inadecuada de privilegios de acceso
	No control de la instalación de *software*
	Interfaces de usuario complejas
	Falta de documentación
	Configuración incorrecta de parámetros
	No sincronización de relojes
	Falta de mecanismos para identificación y autenticación de usuarios
	Tablas de contraseña desprotegidas
	Gestión deficiente de usuarios y claves
	Habilitación de servicios innecesarios
	Uso de *software* nuevo o inmaduro
	No existencia de procesos para el control de cambios
	Uso no controlado de *software*
	Falta de copias de respaldo
	Ausencia de protecciones en las instalaciones físicas en puertas y ventanas
	Falla en la producción de reportes de gestión
Redes	Ausencia de trazabilidad en el envío o recepción de mensaje
	Líneas de comunicación desprotegidas
	Tráfico de datos sensibles no protegido
	Conexión deficiente de los cables
	Puntos únicos de falla
	Falla en la identificación de transmisor y/o receptor
	Arquitectura de red insegura

	Transferencia de contraseñas sin protección
	Gestión inadecuada de la red
	Conexiones a redes públicas sin protección
Personal	Ausencia de personal
	Procedimientos de selección y contratación de personal inadecuado
	Falta de entrenamiento en seguridad de la información
	Ausencia de conciencia en seguridad de la información
	Falta de mecanismos de monitoreo de personal
	Ausencia o desconocimiento de políticas de uso correcto de activos de información
Instalaciones	Uso deficiente de controles de acceso a las instalaciones
	Ubicación en una área susceptible a inundación
	Redes eléctricas inestables
	Ausencia de controles físicos en las instalaciones
Organización	Ausencia de procedimientos formales para registro y retiro del registro de usuarios
	Ausencia de procedimientos formales para revisión de los derechos de acceso
	Ausencia o deficiencia en controles de seguridad de la información en contratos con terceros
	Falta de procedimientos formales para el monitoreo de los recursos de procesamiento de información
	Ausencia de auditorías regulares
	Falta de procedimiento efectivo para gestión de riesgos
	Falta de reportes sobre fallas en los registros de los usuarios, administradores y operadores.
	Inadecuados tiempos de respuesta para el mantenimiento del servicio
	Falta o insuficiencia en acuerdos de niveles de servicio
	Falta de procedimientos para la gestión de cambios
	Falta de procedimientos para la revisión de la seguridad de la información
	Ausencia de procedimientos para clasificación de información y su tratamiento
	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información
	Inexistencia o insuficiencia de los Planes de continuidad
	Ausencia de procedimientos para el control en el desarrollo de *software*
	Ausencia de cláusulas sobre las responsabilidades de la seguridad de la información en los contratos de funcionarios
	Políticas de seguridad de la información inexistentes o desactualizadas

Tabla 2. Ejemplos de posibles vulnerabilidades de los activos de información

b) Identificación de Riesgos

Se realiza con base en los resultados del Contexto Estratégico en cuanto a los factores internos o externos a la entidad, que pueden ocasionar riesgos que afecten el logro de los objetivos. Dentro de la etapa de identificación, se tendrán en cuenta las siguientes políticas:

- La identificación de los riesgos tomará como base todos los procesos que conforman el Sistema Integrado de Gestión, definidos en el mapa de procesos y los productos del MADR.
- Los cambios en la caracterización de los procesos o en la oferta de nuevos servicios/productos del MADR, deberán ser reportados previamente al Grupo Administración del SIG y esto motivará la revisión y actualización de la matriz de identificación de riesgos.

La redacción de los riesgos debe ser de manera concreta, ejemplo: Incumplimiento del contrato.

Los riesgos identificados se clasifican de acuerdo con los siguientes conceptos:

- ***Riesgo Estratégico:*** Se asocia con la forma en que se administra la entidad. Se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la definición de políticas y el diseño y conceptualización de la entidad.
- ***Riesgos de Imagen***: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.
- ***Riesgos Operativos:*** Son los relacionados con la parte operativa y técnica de la entidad, como riesgos provenientes de deficiencias en los sistemas de información, en la definición de los procesos, en la estructura de la entidad, la desarticulación entre dependencias.
- ***Riesgos Financieros:*** Se relacionan con el manejo de los recursos de la entidad, ejecución presupuestal, elaboración de estados financieros, pagos, manejo de excedentes de tesorería y manejo sobre los bienes de la entidad.
- ***Riesgos legales o de Cumplimiento:*** Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
- ***Riesgos Tecnológicos:*** Se relacionan con la capacidad de la entidad para que la tecnología disponible satisfaga las necesidades actuales y futuras de la entidad y soporte el cumplimiento de la misión
- ***Riesgos seguridad de la información:*** Son aquellos riesgos asociados con la perdida de confidencialidad, integridad y disponibilidad de la información, independientemente del formato en que este presente.
- ***Riesgos de corrupción:*** la posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.

c) Análisis de Riesgos

Busca establecer la probabilidad de ocurrencia de un riesgo y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar. Para efectuar el análisis de los riesgos se hace asignándole una calificación a la probabilidad y el impacto, el cual lo ubica en una zona de riesgo, esta calificación se efectúa de acuerdo a lo siguiente:

Probabilidad

Representa el número de veces que el riesgo se ha presentado en un determinado tiempo o puede presentarse. Su calificación se da de acuerdo a la siguiente tabla:

Probabilidad	Descripción	Comentario
1 Raro	No se ha presentado en los últimos 5 años.	El evento puede ocurrir solo en circunstancias excepcionales.
2 Improbable	Al menos de 1 vez en los últimos 5 años.	El evento puede ocurrir en algún momento
3 Posible	Al menos de 1 vez en los últimos 2 años.	El evento podría ocurrir en algún momento
4 Probable	Al menos de 1 vez en el último año.	El evento probablemente ocurrirá en la mayoría de las circunstancias
5 Casi Seguro	Más de 1 vez al año.	Se espera que el evento ocurra en la mayoría de las circunstancias

Tabla 3. Calificación de probabilidad

Impacto

El impacto hace referencia a la magnitud de sus efectos que puede causar un riesgo

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

Tabla 4. Calificación de impacto

Para los riesgos de corrupción el impacto puede tener cualquiera de los siguientes valores: moderado (3), mayor (4) o catastrófico (5). Para seleccionar la opción adecuada (cuando no se tenga claridad), se puede hacer uso del siguiente cuestionario:

Nº Pregunta	Respuesta	
	SI	NO
Si el riesgo de corrupción se materializa podría...		
1 ¿Afectar al grupo de funcionarios del proceso?		

2 ¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3 ¿Afectar el cumplimiento de misión de la Entidad?		
4 ¿Afectar el cumplimiento de la misión del sector al que pertenece la Entidad?		
5 ¿Generar pérdida de confianza de la Entidad, afectando su reputación?		
6 ¿Generar pérdida de recursos económicos?		
7 ¿Afectar la generación de los productos o la prestación de servicios?		
8 ¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?		
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?		
Criterio: si del total de las preguntas... a) **Responde afirmativamente de UNO a CINCO pregunta(s) genera un impacto Moderado.** b) **Responde afirmativamente de SEIS a ONCE preguntas genera un impacto Mayor.** c) **Responde afirmativamente de DOCE a DIECIOCHO preguntas genera un impacto Catastrófico.**		

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

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

Impacto	Criterio Cuantitativo	Criterio Cualitativo
Catastrófico	✓ 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.
Mayor	✓ Impacto que afecte la ejecución presupuestal en un valor ≥20% y menor al 49% ✓ Pérdida de cobertura en la prestación de los servicios de la entidad ≥20% y menor al 49% ✓ Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20% y menor al 49% ✓ Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% y menor al 49%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 ente de control u otro ente regulador. Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. ✓ Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos
Moderado	✓ Impacto que afecte la ejecución presupuestal en un valor ≥5% y menor al 20% ✓ Pérdida de cobertura en la prestación de los servicios de la entidad ≥10% y menor al 19% ✓ Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5% y menor al 19% ✓ Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador,	✓ 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

	las cuales afectan en un valor ≥5% y menor al 19% del presupuesto general de la entidad.	en la prestación del servicio a los usuarios o ciudadanos. ✓ Investigaciones penales, fiscales o disciplinarias.
Menor	✓ Impacto que afecte la ejecución presupuestal en un valor ≤1% y menor al 4% ✓ 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 presupuesto 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.
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 6. Criterios para evaluar el impacto en los riesgos de seguridad de la información

Los criterios anteriores puede usarse dependiendo de la información que posea al momento de la evaluación y estos están asociados con las consecuencias que pueden generar.

Evaluación del riesgo

Permite comparar los resultados de la calificación del riesgo, con los criterios definidos para establecer el grado de exposición de la entidad; de esta forma es posible distinguir entre los riesgos aceptables, tolerables, moderados, importantes o inaceptables y fijar las prioridades de las acciones requeridas para su tratamiento.

Para facilitar la calificación y evaluación de los riesgos, se toman los valores de probabilidad o impacto de las siguientes tablas:

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

Tabla 7. Matriz de evaluación y calificación de riesgos institucionales

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

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

Tabla 8. Matriz de evaluación y calificación para los riesgos de corrupción

Para realizar la evaluación del riesgo, se deben aplicar los siguientes criterios:

- Si el riesgo se ubica en *Zona de Riesgo Baja, Moderado o Alta*, la entidad puede asumirlo, es decir, que el riesgo se encuentra en un nivel que puede aceptarlo sin necesidad de tomar otras medidas de control diferentes a las que se poseen.

- Si el riesgo se ubica en la *Zona de Riesgo Extrema,* se deben implementar controles de prevención para evitar la *Probabilidad* del riesgo, de protección para disminuir el *Impacto* o compartir o transferir el riesgo, si es posible, a través de pólizas de seguros u otras opciones que estén disponibles.

Nota:

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

Valoración del Riesgo:

El objetivo de esta etapa es tomar medidas de control como respuesta al riesgo al que se ve expuesto el MADR. Para ello debe:

a) Identificar controles para el riesgo

Los responsables de los procesos deben establecer los controles, las acciones concretas para aplicar el control, definir los responsables de aplicar el control y la forma de hacer seguimiento a la aplicación de este. Al momento de elaborar el mapa de riesgos se verificará sí los controles están documentados. En el siguiente cuadro se pueden observar algunos ejemplos de distintos tipos de control:

CLASIFICACIÓN	TIPO DE CONTROL
Controles de Gestión	Políticas claras aplicadas Seguimiento al plan estratégico y operativo Indicadores de gestión Tableros de control Seguimiento al cronograma Evaluación del desempeño Informes de gestión Monitoreo de riesgos
Controles Operativos	Conciliaciones Consecutivos Verificación de firmas Listas de chequeo Registro controlado Segregación de funciones Niveles de autorización Custodia apropiada Procedimientos formales aplicados Pólizas Seguridad física Contingencias y respaldo Personal capacitado Aseguramiento y calidad
Controles Legales	Normas claras y aplicadas Control de términos

Tabla 9. Ejemplos de tipos de control

NOTA: Los procesos que hayan identificado riesgos que no posean controles, deben diseñarlos para evitar la materialización del riesgo o generar acciones preventivas para eliminar la causa del posible riesgo. Cuando los controles hayan sido diseñados o las acciones preventivas formuladas se constituyan en controles, el responsable

del proceso informará al Administrador del SIG, para que éste proceda a incluirlo en el Mapa de Riesgos del Proceso.

Para los riesgos de **"seguridad de la información"**, se deben considerar en los controles a implementar, que sean pertinentes y eficaces frente a la protección de la información. Los controles para el tratamiento de los riesgos, se pueden seleccionar de estándares y buenas prácticas como: Magerit, ISO 27001, ISO 27002, COBIT, ITIL u otras fuentes a juicio del responsable de la gestión y tratamiento del riesgo de seguridad de la información

Los controles identificados los podemos clasificar en:

- ***Preventivos:*** son aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización.
- ***Correctivos:*** son aquellos que permiten el restablecimiento de la actividad después de ser detectado un evento no deseable; también permiten la modificación de las acciones que propiciaron su ocurrencia.

b) Verificar la efectividad de los Controles

Para determinar la valoración cuantitativa sobre la efectividad de los controles se hace aplicando el siguiente criterio a cada uno de los controles identificados:

CRITERIO DE EVALUACION	*PARAMETRO DE CALIFICACIÓN*	*PUNTAJE*
1. El control reduce ¿probabilidad o impacto?	Se selecciona "probabilidad" o "impacto"	N/A
2. ¿Existe un mecanismo que le permita llevar un seguimiento sobre este control?	Se selecciona una respuesta: "Sí" o "No"	No → 0 Sí → 15
3. ¿El mecanismo de seguimiento diseñado está documentado a través de instructivos, procedimientos u otro tipo de documento?	Se selecciona una respuesta: "Sí" o "No"	No → 0 Sí →15
4. ¿En el tiempo que lleva el control ejecutándose ha demostrado ser efectivo?	Se selecciona una respuesta: "Sí" o "No"	No → 0 Sí →30
5. ¿Están definidos los responsables de la ejecución y el seguimiento del control?	Se selecciona una respuesta: "Sí" o "No"	No → 0 Sí →15
6. ¿La frecuencia de ejecución del control y seguimiento es adecuada?	Se selecciona una respuesta: "Sí" o "No"	No → 0 Sí →25

Tabla 10. Valoración de controles

Para cada control, se determina si reduce probabilidad o impacto, se suma los puntajes (de los criterios 2 al 6 de la tabla anterior) y se establece el desplazamiento en la Matriz De Evaluación y Calificación de Riesgos, de acuerdo al siguiente criterio:

RANGO DE CALIFICACIÓN DE LOS CONTROLES	***CUADRANTES A DISMINUIR EN LA MATRIZ DE EVALUACION Y CALIFICACIÓN DE RIESGOS***	
	PROBABILIDAD	IMPACTO
Entre 0 -50	0	0
Entre 51-75	1	1
Entre 76-100	2	2

Tabla 11. Matriz de evaluación y calificación de Riesgos

Una vez valorado cada uno de los controles, se totaliza los cuadrantes a desplazar tanto en probabilidad y como en impacto, y se procede a hacer el desplazamiento en la Matriz de Evaluación y Calificación de Riesgos. La nueva posición corresponde al riesgo residual.

Es responsabilidad del dueño del proceso garantizar que los controles definidos se aplican y son efectivos, y la administración del SIG hará mínimo una revisión al año a los mapas de riesgos de todos los procesos, con el fin de garantizar que se actualiza los controles y no se hayan materializado los riesgos.

Como complemento se hace una verificación aleatoria de los riesgos, por la Oficina de Control Interno a través de una auditoria.

c) Establecer tratamiento

Una vez evaluados los controles y establecido el riesgo residual, se procede a establecer el tratamiento a los riesgos residuales, el cual puede ser:

- **Evitar el riesgo**, tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas.

  Por ejemplo: el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.

- **Reducir el riesgo**, implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles.

  Por ejemplo: a través de la optimización de los procedimientos y la implementación de controles

- **Compartir o transferir el riesgo**, reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido.

  Por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar, la tercerización.

- **Asumir un riesgo**, luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso, el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.