GUÍA METODOLÓGICA PARA LA IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS

PROCESO

ADMINISTRACION DEL SISTEMA INTEGRADO DE GESTIÓN

Versión 1

13/12/2016

Contenido

1. PRESENTACIÓN

El Ministerio de Ambiente y Desarrollo Sostenible como entidad del orden público se encuentra expuesta a una serie de factores de tipo externo e interno que pueden poner en riesgo el cumplimiento de su misión y objetivos institucionales, así como el desarrollo eficiente y efectivo de sus procesos; por ende se hace necesario realizar el análisis del contexto e implementar una guía metodológica que permita identificar, evaluar, valorar y definir el tratamiento encaminado al manejo de los impactos generados.

Es importante así mismo el cumplimiento de requisitos de orden normativo contemplados a través del Decreto 1537 de 2001 en donde se establece la identificación y el análisis de riesgos como un proceso permanente e interactivo entre las oficinas de control interno y la administración, y deja a la vista la responsabilidad que deben adquirir los encargados de los procesos en la aplicación de las políticas de tratamiento definidas. En este sentido, el Decreto 1599 de 2005 adopta el Modelo Estándar de Control Interno – MECI para todas las entidades del Estado, en donde se contempla a la administración del riesgo dentro del Subsistema de Control Estratégico. Valiéndose de elementos como la misión, la visión, los objetivos, los valores y las estrategias para promover el compromiso de la dirección e involucrarse en todos los procesos de la entidad, Este modelo fue actualizado a través del decreto 943 de 2014.

Por otra parte, una vez la entidad estructure su sistema de administración de riesgos, éste: contribuye al logro de los objetivos institucionales y al mejoramiento del desempeño organizacional a través de la generación de una cultura del riesgo, define una base confiable para la planeación y la toma de decisiones, involucra a todos los procesos y el talento humano de la entidad y promueve el mejoramiento continuo a partir del seguimiento, la revisión y el establecimiento de metas de desempeño institucional, dirigidas a mejorar la calidad de los productos y servicios ofertados y la eficacia de las operaciones realizadas.

A continuación se describen las etapas para la identificación, análisis, evaluación y tratamiento de los riesgos vinculados con los procesos del Sistema Integrado de Gestión del MADS y aquellos que por disposición de la ley 1474 de 2011 son denominados riesgos de corrupción.

2. OBJETIVO

Establecer los lineamientos metodológicos para llevar a cabo la identificación y valoración de riesgos por procesos con miras a generar el Mapa de Riesgos del Ministerio de Ambiente y Desarrollo Sostenible.

3. ALCANCE

Esta guía es aplicable a los procesos Estratégicos, Misionales, de Apoyo y de Evaluación Independiente del Ministerio de Ambiente y Desarrollo Sostenible para todos los subsistemas que conforman el Sistema Integrado de Gestión.

4. DEFINICIONES Y/O CONCEPTOS

- **ACTIVO:** Recursos del sistema de información o relacionados con este, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por la dirección. “Cualquier cosa que tenga valor para la organización” ISO 27000:2014

- **ADMINISTRACIÓN DE RIESGOS:** Conjunto de Elementos de Control que al interrelacionarse permiten a la Entidad Pública evaluar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos, que permitan identificar oportunidades para un mejor cumplimiento de su función. (MECI 1000:2005).

- **ANÁLISIS DEL RIESGO**: Elemento de Control, que permite establecer la probabilidad de ocurrencia de los eventos positivo y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la Entidad Pública para su aceptación y manejo.

- **AMENAZA:** Una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización. ISO 27000:2014.

- **CONFIDENCIALIDAD:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. ISO 27000:2014.

- **CONSECUENCIA:** Resultado de un evento expresado cualitativa o cuantitativamente, sea este una pérdida, perjuicio, desventaja o ganancia, frente a la consecución de los objetivos de la entidad o el proceso.

- **CONTEXTO ESTRATÉGICO**: Elemento de Control, que permite establecer el lineamiento estratégico que orienta las decisiones de la Entidad Pública, frente a los riesgos que pueden afectar el cumplimiento de sus objetivos producto de la observación, distinción y análisis del conjunto de circunstancias internas y externas que puedan generar eventos que originen oportunidades o afecten el cumplimiento de su función, misión y objetivos institucionales. (MECI 1000:2014).

- **CONTROL:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **CRITERIOS DE RIESGOS:** Términos de referencia sobre los cuales se evalúa la importancia de un riesgo. Estos criterios se definen con base en los objetivos de la organización y en el contexto interno y externo.

- **DISPONIBILIDAD:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. ISO 27000:2014.

- **GESTIÓN DE RIESGOS**: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y tratamiento del riesgo. ISO 27000:2014.

- **IDENTIFICACIÓN DE RIESGOS**: Elemento de Control, que posibilita conocer los eventos potenciales, estén o no bajo el control de la Entidad Pública, que ponen en riesgo el logro de su Misión, estableciendo los agentes generadores, las causas y los efectos de su ocurrencia. (MECI 1000:2005).

- **IMPACTO:** Consecuencias que puede ocasionar a la organización la materialización del riesgo.

- **INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN:** Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **INTEGRIDAD:** Propiedad de la información relativa a su exactitud y completitud. ISO 27000:2014.

- **NIVEL DE RIESGOS:** Comprende la magnitud de un riesgo o la combinación de riesgos, determinado con base en las consecuencias de su ocurrencia y en la probabilidad.

- **POLÍTICAS DE ADMINISTRACIÓN DE RIESGOS**: Elemento de Control, que permite estructurar criterios orientadores en la toma de decisiones, respecto al tratamiento de los riesgos y sus efectos al interior de la Entidad Pública. (MECI 1000:2014).

- **PROBABILIDAD:** Consiste en la posibilidad de ocurrencia del riesgo; ésta puede ser medida con criterios de Frecuencia, si se ha materializado o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado.

- **PROCESO:** Sistema de actividades que utilizan recursos para transformar entradas en salidas.

- **PROPIETARIO DEL RIESGO:** Persona o entidad con responsabilidad y autoridad para gestionar un riesgo

- **RIESGO:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos, los proceso o los servicios. Se expresa en términos de probabilidad y consecuencias.

- **RIESGO INHERENTE:** Es aquel al que se enfrenta una entidad en su ausencia de acciones de la dirección para modificar su probabilidad o impacto.

- **RIESGO RESIDUAL:** Nivel de riesgo que permanece luego de tomar medidas de tratamiento o controles del riesgo.

- **VALOR DEL ACTIVO**: Está determinado por el valor de la confidencialidad, integridad y disponibilidad del activo de información.

- **VALORACIÓN DEL RIESGO**: Elemento de Control, que determina el nivel o grado de exposición de la Entidad Pública a los impactos del riesgo, permitiendo estimar las prioridades para su tratamiento. (MECI 1000:2014).

- **VULNERABILIDAD:** Debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas. ISO 27000:2014.

5. MARCO REGULATORIO O NORMATIVO

- Ley 87 de 1993.
- Ley 489 de 1998.
- Ley 1474 de 2011.
- Decreto 943 de 2014.
- Decreto 1537 de 2001.
- Decreto 2145 de 1999.
- Decreto 2593 de 2000.
- Directiva Presidencial 09 de 1999.
- Decreto 1599 de 2005.
- Decreto 4485 de 2009.
- MECI 1000:2014
- NTCGP 1000:2009
- NTC ISO 31000:2011
- NTC ISO 27005:2008
- NTC ISO 27001:2013
- NTC ISO 27002:2013
- Plan Anticorrupción y de Atención al Ciudadano -MADS
- Guía Para La Gestión Del Riesgo De Corrupción 2015 –Presidencia de la República
- Guía Para La Administración Del Riesgo -DAFP

6. RESPONSABILIDAD

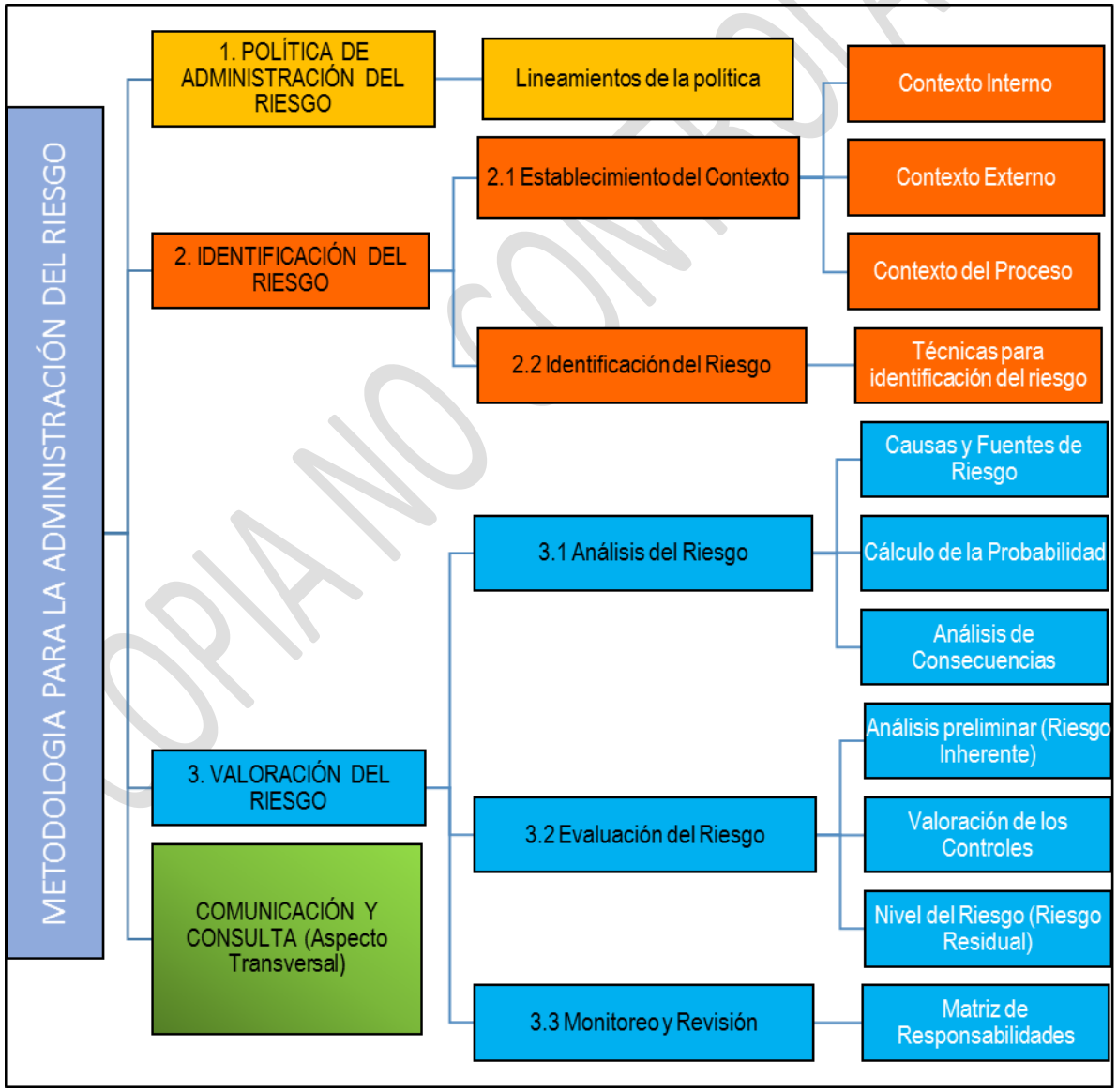
Todos los líderes de los procesos definidos en el Sistema Integrado de Gestión del ministerio serán responsables de la aplicación de esta metodología, la implementación de los controles definidos y su seguimiento, con el apoyo permanente de la Oficina Asesora de Planeacion.

Así mismo, la Oficina de Control Interno verificara el cumplimiento e implementación de esta guía en los procesos definidos por la entidad y la medición de la eficacia de las acciones y controles que permitan contrarrestar la materialización de los riesgos identificados. Para el establecimiento e implementación de un Sistema de Administración de Riesgos es necesario contar con el compromiso y la definición de responsabilidades desde el Despacho del Ministerio y Viceministerio de Ambiente y Desarrollo Sostenible hacia todos los niveles de la entidad.

Para esto, la alta dirección de acuerdo con lo establecido en la Guía Metodológica para la Identificación y Valoración de Riesgos, debe designar al representante de la alta dirección y al equipo MECI para apoyar a los líderes de procesos y demás servidores quienes son en última instancia los encargados de identificar y elaborar el mapa de riesgo.

7. METODOLOGIA PARA LA ADMINISTRACIÓN Y GESTIÓN DEL RIESGOS.

Esquema 1: Metodología para la Administración del Riesgo



7.1 POLITICA DE ADMINISTRACIÓN Y GESTIÓN DE RIESGOS

La Alta Dirección del Ministerio de Ambiente y Desarrollo Sostenible en conocimiento de la responsabilidad e importancia del manejo de los riesgos asociados a los diferentes procesos del Sistema Integrado de Gestión, implementa esta Guía Metodológica a través del aplicativo del MADSIGestión para la Identificación y Valoración de Riesgos por procesos como herramienta estratégica y de gestión que permita anticipar y responder de manera oportuna y optima a la materialización de los riesgos identificados en la matriz, contribuyendo al cumplimiento de los objetivos misionales y la mejora continua del sistema.

Así mismo, la Política de Administración y Gestión de Riesgos será publicada y comunicada a todos los funcionarios y colaboradores del Ministerio de Ambiente y Desarrollo Sostenible a través de los diferentes medios con que cuenta la entidad.

7.1.2 OBJETIVOS DE LA POLÍTICA

- Controlar a través de MADSIGestión todo el proceso relacionado con el manejo de los riesgos asociados al Sistema Integrado de Gestión. (Matriz de Riesgos).
- Proporcionar al Ministerio las directrices para la administración de los riesgos asociados a los procesos de la entidad, con el propósito de contribuir a la adecuada identificación, análisis, valoración (riesgos y controles) y tratamiento de los mismos.
- Integrar en una sola metodología el manejo los riesgos de gestión, corrupción, ambientales y seguridad de la información.
- Establecer la responsabilidad de los diferentes líderes de los procesos del ministerio.
- Establecer el rol de los diferentes grupos de trabajo del Ministerio.
- Dar cumplimiento a los requerimientos legales que apliquen al manejo de riesgos de gestión, corrupción, ambientales y de seguridad de la información.
- Servir para el comportamiento profesional y personal de los funcionarios de Minambiente

7.2 IDENTIFICACIÓN DEL RIESGO

En esta etapa se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas. (NTC ISO31000, Numeral 2.15).

Elementos que lo conforman: Establecimiento del Contexto e Identificación del Riesgo

7.2.1 ESTABLECIMIENTO DEL CONTEXTO

Corresponde a la definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo. (NTC ISO31000, Numeral 2.9)

De igual manera, todas las actividades internas y del entorno, que pueden generar eventos que originan oportunidades o afecten negativamente el cumplimiento de la misión y objetivos de una institución.

CONTEXTO EXTERNOS: Se determinan las características o aspectos esenciales del entorno en el cual opera la entidad	ECONÓMICOS**: Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia**
	MEDIOAMBIENTALES: Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible
	POLÍTICOS: Cambios de gobierno, legislación, políticas públicas, regulación
	SOCIALES: Demografía, responsabilidad social, terrorismo.
	TECNOLÓGICOS: Avances en tecnología, acceso a sistemas de información externos, gobierno en línea, requisitos de partes interesadas externas seguridad de la información.
	COMUNICACIÓN EXTERNA: Mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad
CONTEXTO INTERNOS: Se determinan las características o aspectos esenciales del ambiente en cual la organización busca alcanzar sus objetivos.	**FINANCIEROS:** Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada
	PERSONAL: Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional
	PROCESOS: Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
	TECNOLOGÍA: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información, requisitos de partes interesadas internas seguridad de la información.
	ESTRATÉGICOS: Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo
	COMUNICACIÓN INTERNA: Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de todos los procesos de la entidad.
CONTEXTO DEL	**DISEÑO DEL PROCESO:** Claridad en la descripción del alcance y objetivo del proceso.

PROCESO: Se determinan las características o aspectos esenciales del proceso y sus interrelaciones.	**INTERACCIONES CON OTROS PROCESOS:** Relación precisa con otros procesos en cuanto insumos, proveedores, productos, usuarios o clientes.
	TRANSVERSALIDAD: Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
	PROCEDIMIENTOS ASOCIADOS: Pertinencia en los procedimientos que desarrollan los procesos.
	RESPONSABILIDAD DEL PROCESO: Grado de autoridad y responsabilidad de los funcionarios frente al proceso.
	COMUNICACIÒN ENTRE LOS PROCESOS: Efectividad en los flujos de información determinados en la interacción de los procesos.

Fuente: DAFP

7.2.2 IDENTIFICACIÓN DE RIESGOS

La identificación del ***riesgo de gestión*** se realiza determinando las causas, con base en el contexto interno, externo y del proceso ya analizado para el ministerio, y que pueden afectar el logro de los objetivos. Algunas causas externas no controlables por la entidad se podrán evidenciar en el análisis de contexto correspondiente, para ser tenidas en cuenta en el análisis y valoración del riesgo.

A partir de ese levantamiento de causas se procederá a identificar el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso, es necesario referirse a sus características o las formas en que se observa o manifiesta. En este caso es posible hacer una corta descripción del riesgo dentro de la identificación,

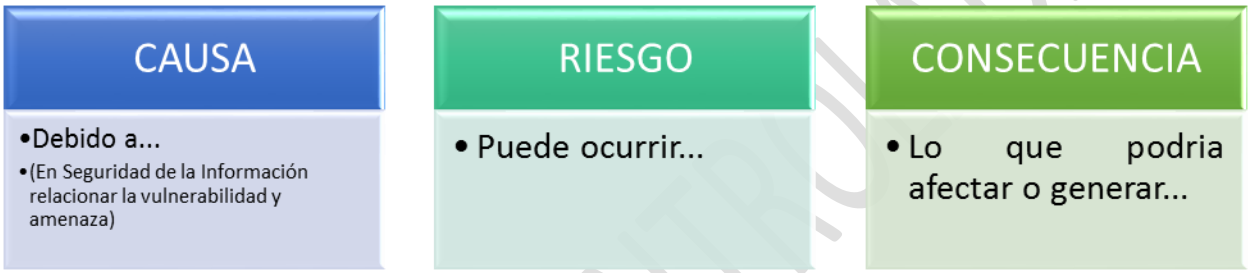
Para identificar ***riesgos en seguridad*** de la información de una manera asertiva es importante verificar posibles hechos que afecten la disponibilidad, integridad y/o confidencialidad de la información, esto tanto a nivel físico y/o lógico, hardware, software, a nivel de instalaciones locativas o legales que lleven a afectar la información de la entidad o la privacidad de la información de una parte interesada.

Es también importante identificar las causas que originan el riesgo en base a la identificación de vulnerabilidades y amenazas. La Identificación de las vulnerabilidades de los activos de información son debilidades que son aprovechadas por amenazas y generan un riesgo, una vulnerabilidad que no tiene una amenaza, puede no requerir de la implementación de un control, para lo cual es necesario identificarla y monitorear. Pero es necesario dejar claro que un control mal diseñado e implementado puede constituir una vulnerabilidad.

Las amenazas son de origen natural o humano y pueden ser accidentales o deliberadas, algunas amenazas pueden afectar a más de un activo generando diferentes impactos. Dentro de algunas amenazas dentro de la norma ISO 27005:2008 son consideradas: Virus informático y software

malicioso, avería de origen físico, errores de monitorización (log's), errores de usuarios, corte de suministro eléctrico, fallas eléctricas, daños por agua, fallo de comunicaciones, degradación de los soportes principales de almacenamiento de información, fenómeno natural, derrame de líquidos o sólidos, fuego, entre otras.

Para llevar a cabo este proceso se recomienda dar respuesta a los siguientes interrogantes:



CLASES DE RIESGOS

Para la identificación de los riesgos y con el objeto de incorporar toda clase de riesgo asociado con el proceso, con la seguridad de la información y con el ambiente, se puede tener en cuenta la siguiente clasificación dada por el Departamento Administrativo de la Función Pública y complementada a través de la Guía para la Administración del Riesgo:

- **RIESGO ESTRATÉGICO:** se asocia con la forma en que se administra la Entidad, su manejo se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

- **RIESGO DE IMAGEN**: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

- **RIESGOS OPERATIVOS:** Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de procesos, de la estructura de la entidad, de la articulación entre dependencias.

- **RIESGOS FINANCIEROS:** Se relacionan con el manejo de los recursos de la entidad que incluyen la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

- **RIESGOS 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 DE TECNOLOGÍA**: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

- **RIESGO DE CORRUPCIÓN:** 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.

- **RIESGO DE SEGURIDAD DE LA INFORMACIÓN**: Potencial de que una amenaza determinada explore las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. ISO 27000:2014.

- **RIESGOS AMBIENTALES:** Están relacionados con la posibilidad de que se genere un daño al ambiente como consecuencia del desarrollo de las actividades realizadas en la entidad

7.3 VALORACION DEL RIESGO

Consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial. (RIESGO INHERENTE).

Elementos que lo conforman: Análisis del Riesgo, Valoración del Riesgo y Monitoreo y Revisión

7.3.1 ANÁLISIS DEL RIESGO

DETERMINAR PROBABILIDAD

Por **PROBABILIDAD** se entiende la posibilidad de ocurrencia del riesgo, ésta puede ser medida con criterios de Frecuencia o Factibilidad.

Bajo el criterio de **FRECUENCIA** se analizan el # eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo

Bajo el criterio de **FACTIBILIDAD** se analiza la presencia de factores internos y externos que pueden proporcionar el riesgo, se trata en este caso de un hecho que no se ha presentado pero es posible que se dé.

Para su determinación se utiliza la tabla de probabilidad No1:

Tabla No1: Tabla de Probabilidad Riesgos del Sistema Integrado de Gestión

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

DETERMINAR NIVEL DE IMPACTO O CONSECUENCIAS

Por **IMPACTO** se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Para su determinación el nivel de impacto o consecuencias de los **RIESGOS DE GESTIÓN** se utiliza la tabla de probabilidad No2:

Tabla No2: Tabla de Medición del Impacto o Consecuencias de Riesgos del Sistema Integrado de Gestión de Calidad

NIVELES	IMPACTO (CONSECUENCIAS) CUALITATIVO
CATASTRÓFICO	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 de 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.

	La publicación no autorizada o fuga de información puede llevar a sanciones para la entidad y afectación de la imagen institucional.
MAYOR	Interrupción de las operaciones de la Entidad por más de dos (2) días.
	Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta
	Sanción por parte del ente de control u otro ente regulador
	Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno.
	Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos
	La publicación no autorizada, acceso no autorizado o fuga de información puede afectar la imagen institucional.
MODERADO	Interrupción de las operaciones de la Entidad por un (1) día
	Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad.
	Inoportunidad en la información ocasionando retrasos en la atención a los usuarios
	Reproceso de actividades y aumento de carga operativa.
	Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación de servicios a los usuarios o ciudadanos
	Investigaciones penales, fiscales o disciplinarias
	La publicación no autorizada, acceso no autorizado o fuga de información puede afectar un proceso u ocasionar investigaciones o sanciones internas.
MENOR	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
	La publicación no autorizada, acceso no autorizado o fuga de información puede afectar de manera leve a un proceso en particular.
INSIGNIFICANTE	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.
	La publicación no autorizada, acceso no autorizado o fuga de información no afecta a la entidad.

Para su determinación el nivel de impacto o consecuencias de los **RIESGOS DE CORRUPCIÓN** se utiliza la tabla de probabilidad No3:

Tabla No3: Tabla de Preguntas para la Medición del Impacto de Riesgos de Corrupción

FORMATO PARA DETERMINAR EL IMPACTO			
No	**PREGUNTA**	**RESPUESTA**	
Si el riesgo de corrupción se materializa podría…		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 la misión de la entidad		
4	Afectar el cumplimiento de la misión del sector a la 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 de la entidad		
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 proceso 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		

Por lo anterior, y teniendo en cuenta las respuestas a las preguntas referentes a la valoración de los riesgos de corrupción se establece la siguiente valoración:

Tabla No4: Tabla de Medición del Impacto de los Riesgos de Corrupción

NIVEL	IMPACTO	DESCRIPCIÓN	RIESGOS DE CORRUPCIÓN
1	INSIGNIFICANTE	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad y el proceso.	No Aplica
2	MENOR	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad y el proceso.	No Aplica
3	MODERADO	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad y el proceso.	Responder afirmativamente de UNO a CINCO pregunta(s) genera un impacto **MODERADO**
4	MAYOR	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad y el proceso.	Responder afirmativamente de SEIS a ONCE preguntas genera un impacto **MAYOR**
5	CATASTRÓFICO	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad y el proceso.	Responder afirmativamente de DOCE a DIECIOCHO preguntas genera un impacto **CATASTRÒFICO**

Tratándose de Riesgos de Corrupción el impacto siempre será negativo; en este orden de ideas no aplica la descripción de ***riesgos insignificante o menores.***

ESTIMAR EL NIVEL DEL RIESGO INICIAL

Se logra a través de la determinación de la probabilidad y el impacto que puede causar la materialización del riesgo, a través de las tablas establecidas en cada uno. Para su determinación se utiliza la Matriz de Calificación del Riesgo No1

Matriz No1: Matriz de Calificación, Evaluación y Respuesta a los Riesgos:

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

B: **Zona de riesgo Baja**: Asumir el riesgo.
M: **Zona de riesgo Moderada**: Asumir el riesgo, reducir el riesgo.
A: **Zona de riesgo Alta**: Reducir el riesgo, evitar, compartir o transferir
E: **Zona de riesgo Extrema**: Reducir el riesgo, evitar, compartir o transferir
Nota: Este primer análisis del riesgo se denomina ***Riesgo Inherente*** y se define como aquél al que se enfrenta una entidad en ausencia de acciones por parte de la Dirección para modificar su probabilidad o impacto

7.3.2 EVALUACIÓN DEL RIESGO

Se busca confrontar los resultados del análisis del riesgo inicial (INHERENTE) frente a los controles establecidos, con el fin de determinar la zona de riesgo final (RESIDUAL).

Riesgo inicial (Inherente) – Efecto de los controles = Riesgo Final (Residual)

Para realizar el análisis y la valoración de los controles existentes es necesario:

DETERMINAR SU NATURALEZA:

Si se trata de un control preventivo, detectivo o correctivo

CONTROLES PREVENTIVOS: Aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización.

Evitan que un evento suceda. Por ejemplo el requerimiento de un login y pasword en un sistema de información es un control preventivo. Este previene (teóricamente) que personas no autorizadas puedan ingresar al sistema.

CONTROLES CORRECTIVOS: Aquellos que se implementan una vez se materializa el riesgo y que permiten el restablecimiento de la actividad.

Estos no prevén que un evento suceda, pero permiten enfrentar la situación una vez se ha presentado. Por ejemplo en caso de un desastre natural u otra emergencia mediante las pólizas de seguro y otros mecanismos de recuperación de negocio respaldo, es posible volver a recuperar las operaciones

CONTROLES DISUASIVOS: Estos controles reducen la probabilidad de un ataque deliberado.

CONTROLES DETECTIVOS: Son aquellos que no evitan que ocurran las causas del riesgo sino que los detecta luego de ocurridos. Por lo que permiten registrar un evento después de que ha sucedido, por ejemplo, registro de las entradas de todas las actividades llevadas a cabo en un sistema de información, traza de los registros realizados, de las personas que ingresaron, entre otros

DETERMINAR SI LOS CONTROLES ESTÁN DOCUMENTADOS

De forma tal que es posible conocer cómo se lleva a cabo el control, quien es el responsable de su ejecución, lo cual determinará las evidencias que van a respaldar la ejecución del mismo.

ESTABLECER SI EL CONTROL QUE SE IMPLEMENTA ES AUTOMÁTICO O MANUAL

CONTROLES AUTOMÁTICOS: Utilizan herramientas tecnológicas como sistemas de información o software que permiten incluir contraseñas de acceso, o con controles de seguimiento a aprobaciones o ejecuciones que se realizan a través de éste, generación de reportes o indicadores, sistemas de seguridad con scanner, sistemas de grabación, entre otros. Este tipo de controles suelen ser más efectivos en algunos ámbitos dada su complejidad.

CONTROLES MANUALES: Políticas de operación aplicables, autorizaciones a través de firmas o confirmaciones vía correo electrónico, archivos físicos, consecutivos, listas de chequeo, controles de seguridad con personal especializado, entre otros.

DETERMINAR SI LOS CONTROLES SE ESTÁN APLICANDO EN LA ACTUALIDAD.

Y si han sido efectivos para minimizar el riesgo. Para realizar dicho análisis, a continuación se muestra la tabla de análisis y evaluación, con el fin de calificar de forma objetiva los controles y de este modo poder determinar el desplazamiento dentro de la matriz de evaluación de riesgos.

Nota: Las calificaciones planteadas para cada aspecto deben ser usadas tal como están expresadas, aplicar el valor asignado a cada aspecto si responde SI; cero (0) si responde NO. No se asignaran valores intermedios para evitar subjetividad en el análisis.

Tabla No5: Tabla de Análisis y Evaluación de los Controles

Criterios para la evaluación	EVALUACIÓN		Observaciones
	Si	No	
¿El Control previene la materialización del riesgo. (Afecta probabilidad)? ¿El control permite enfrentar la situación en caso de materialización (Afecta impacto)?	N/A	N/A	Este criterio no puntúa, es relevante determinar si el control es preventivo (probabilidad) o si es correctivo que permite enfrentar el evento una vez materializado (impacto), con el fin de establecer el desplazamiento en la matriz de evaluación de riesgos.
Existen manuales, instructivos o procedimientos para el manejo del control	15	0	
Está(n) definido(s) el(los) responsable(s) de la ejecución del control y del seguimiento	5	0	
El control es automático	15	0	
El control es manual	10	0	
La frecuencia de la ejecución del control y seguimiento es adecuada	15	0	
Se cuenta con evidencia de la ejecución y seguimiento del control	10	0	
En el tiempo que lleva la herramienta ha demostrado ser efectiva	30	0	
TOTAL	**100**		

Una vez realizada la valoración del riesgo se comparan los resultados obtenidos del riesgo inicial (inherente) con los controles establecidos, para establecer la zona de riesgo final (residual). Se califica de acuerdo a la siguiente tabla:

Tabla No 6: Tabla de disminución de cuadrantes

RANGOS DE CALIFICACIÓN DE LOS CONTROLES	Dependiendo si el control afecta probabilidad o impacto desplaza en la matriz de evaluación del riesgo
	CUADRANTES A DISMINUIR
Entre 0 – 50	0
Entre 51 – 75	1
Entre 76 – 100	2

- Si son identificados más de un control asociado al riesgo, cada uno deberá ser calificado
- Plan de manejo del riesgo: Consiste en definir la manera en la que se implantarán las opciones de manejo del riesgo, estableciendo los responsables, el cronograma de implementación de las acciones y los indicadores para su evaluación.

TRATAMIENTO DEL RIESGO

El tratamiento implica la selección de una o varias opciones para el manejo de los riesgos identificados, evaluados y valorados.

Dentro de las opciones y luego de determinar la zona de riesgo, se pueden contemplar las siguientes:

- **Evitar el riesgo (EV):** Tomar las acciones preventivas necesarias encaminadas a evitar 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. Ejemplo: el control de calidad, manejo de insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.

- **Reducir el riesgo (RE):** Implementar las acciones necesarias para disminuir tanto su probabilidad de ocurrencia (acciones preventivas) como los impactos derivados de su materialización (acciones correctivas). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Ejemplo: a través de la optimización de los procedimientos y la implementación de controles.

- **Compartir o transferir el riesgo (TR):** Consiste en trasladar el riesgo para que sea gestionado por un tercero ajeno a la Entidad, el cual asume el costo en caso de la materialización del evento; así mismo, apoya las medidas de control para reducirlo. Como en el caso de los contratos de seguros o a través de otros medios que permitan distribuir una porción del riesgo con otra entidad, como en los contratos de riesgo compartido. 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 el riesgo (AS):** No tomar medidas preventivas ni correctivas frente al riesgo analizado, debido a que su ocurrencia no tendrá un impacto significativo en la entidad o la probabilidad de que se presente es muy remota.

La selección de una o más opciones de tratamiento, requiere del análisis costo-beneficio, acompañado de elementos como la viabilidad jurídica, técnica e institucional de la opción u opciones a implementar y la aprobación del dueño del proceso o la dirección según sea el caso.

7.3.3 MONITOREO Y REVISIÓN

El monitoreo y revisión debe asegurar que las acciones establecidas en los mapas de riesgo se están llevando a cabo y evaluar la eficiencia en su implementación, así como para determinar si existen cambios en el contexto interno y/o externo, incluyendo los cambios en los criterios de riesgo y en el propio riesgo.

RESPONSABLES DE LOS PROCESOS

Encargados de realizar las acciones asociadas a los controles establecidos para cada uno de los riesgos identificados para su proceso, de acuerdo con la periodicidad establecida en la política de administración del riesgo en la entidad.

Durante la aplicación de las acciones de seguimiento cada líder de proceso debe mantener la traza o documentación respectiva de todas las actividades realizadas, para garantizar de forma razonable que dichos riesgos no se materializarán y por ende que los objetivos del proceso se cumplirán.

OFICINA DE CONTROL INTERNO

Encargada de realizar el seguimiento a los riesgos que a nivel institucional han sido consolidados. En sus procesos de auditoria interna dicha oficina debe analizar el diseño e idoneidad de los controles, determinando si son o no adecuados para prevenir o mitigar los riesgos de los procesos,

haciendo uso de las técnicas relacionadas con pruebas de auditoría que permitan determinar la efectividad de los controles.

En cuanto a la periodicidad del seguimiento, para los riesgos asociados a posibles actos de corrupción, se debe dar cumplimiento a las fechas establecidas por "La Guía para la Gestión del riesgo de Corrupción" de la Presidencia de la Republica." Como se indica a continuación:

El seguimiento se realiza **tres (3) veces al año** en las siguientes fechas:

Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de mayo.

Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de septiembre.

Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de enero.

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en lugar de fácil acceso al ciudadano.

8. COMUNICACIÓN Y CONSULTA

La comunicación y la consulta deberá surtirse en todas las etapas de construcción del mapa de riesgos institucional en el marco de un proceso participativo que involucre actores internos y externos del ministerio.

Esta etapa tiene como principales objetivos los siguientes:

1. Ayudar a establecer el **contexto estratégico**
2. Ayudar a determinar que los **riesgos** estén correctamente identificados.
3. Reunir diferentes **áreas de experticias** para el análisis de los riesgos.
4. Fomentar la **gestión de riesgos**.

Una vez surtido este proceso de consulta es de suma importancia que se comunique internamente el mapa de riesgos institucional y externamente el mapa de riesgos de corrupción. De tal manera que funcionarios y contratistas del ministerio; así como las partes interesadas, conozcan la forma como se estructuran los riesgos de gestión y corrupción.