



**El ambiente
es de todos**

Minambiente

**GUIA DE
ADMINISTRACIÓN DEL
RIESGO**

PROCESO


Administración del Sistema

Integrado de Gestión

Versión 4


31/07/2020

MADSIG
Sistema Integrado de Gestión

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

CONTENIDO

1	PRESENTACIÓN	3
2	OBJETIVO	4
3	ALCANCE	4
4	DEFINICIONES O CONCEPTOS	4
5	MARCO REGULATORIO O NORMATIVO	7
6	RESPONSABILIDAD	7
7	METODOLOGIA PARA LA ADMINISTRACIÓN Y GESTIÓN DEL RIESGOS	8
7.1	POLITICA DE ADMINISTRACIÓN Y GESTIÓN DE RIESGOS	8
7.1.1	OBJETIVOS DE LA POLÍTICA	9
7.2	IDENTIFICACIÓN DEL RIESGO	9
7.2.1	ESTABLECIMIENTO DEL CONTEXTO	9
7.2.2	IDENTIFICACIÓN DE RIESGOS	10
7.3	VALORACION DEL RIESGO	15
7.3.1	ANÁLISIS DEL RIESGO	15
7.3.2	EVALUACIÓN DEL RIESGO	22
7.3.3	TRATAMIENTO DEL RIESGO	27
7.4	MONITOREO Y REVISIÓN	28
7.5	MAPA DE RIESGOS INSTITUCIONAL	31
8	COMUNICACIÓN Y CONSULTA	31

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05


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 de los decretos 943 de 2014 y 1499 de 2017.

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 de MINAMBIENTE y aquellos que por disposición de la ley 1474 de 2011 son denominados riesgos de corrupción.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

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

Apoyar la administración del riesgo en 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 O CONCEPTOS

- **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.

- **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).


- **AMENAZA:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

- **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.

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

- **CONFIDENCIALIDAD:** Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

- **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

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

- **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:** Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

- **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:** Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

- **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:** Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.


- **INCIDENTE:** Evento o serie de eventos de seguridad digital 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.

- **MAPA DE RIESGOS:** Documento con la información resultante de la gestión del riesgo.

- **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).

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

- **PROBABILIDAD:** Se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.

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

- **RIESGO DE SEGURIDAD DIGITAL:** Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

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


- **RIESGO RESIDUAL:** Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.

- **TOLERANCIA AL RIESGO:** Son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

- **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:** Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

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.
- Decreto 1499 de 2017.
- NTC ISO 31000:2011.
- NTC ISO 27000:2014.
- NTC ISO 27001:2013.
- Plan Anticorrupción y de Atención al Ciudadano Ministerio de Ambiente y Desarrollo Sostenible
- Guía Para La Administración del Riesgo y el Diseño de Controles en entidades Públicas-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 Planeación.

Así mismo, la Oficina de Control Interno verificará 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 Viceministerios hacia todos los niveles de la entidad.

Para esto, la alta dirección debe designar al representante de la alta dirección y al equipo SIG para apoyar a los líderes de procesos y demás servidores quienes son en última instancia los encargados de identificar y elaborar el mapa de riesgos.

7 METODOLOGIA PARA LA ADMINISTRACIÓN Y GESTIÓN DEL RIESGOS.

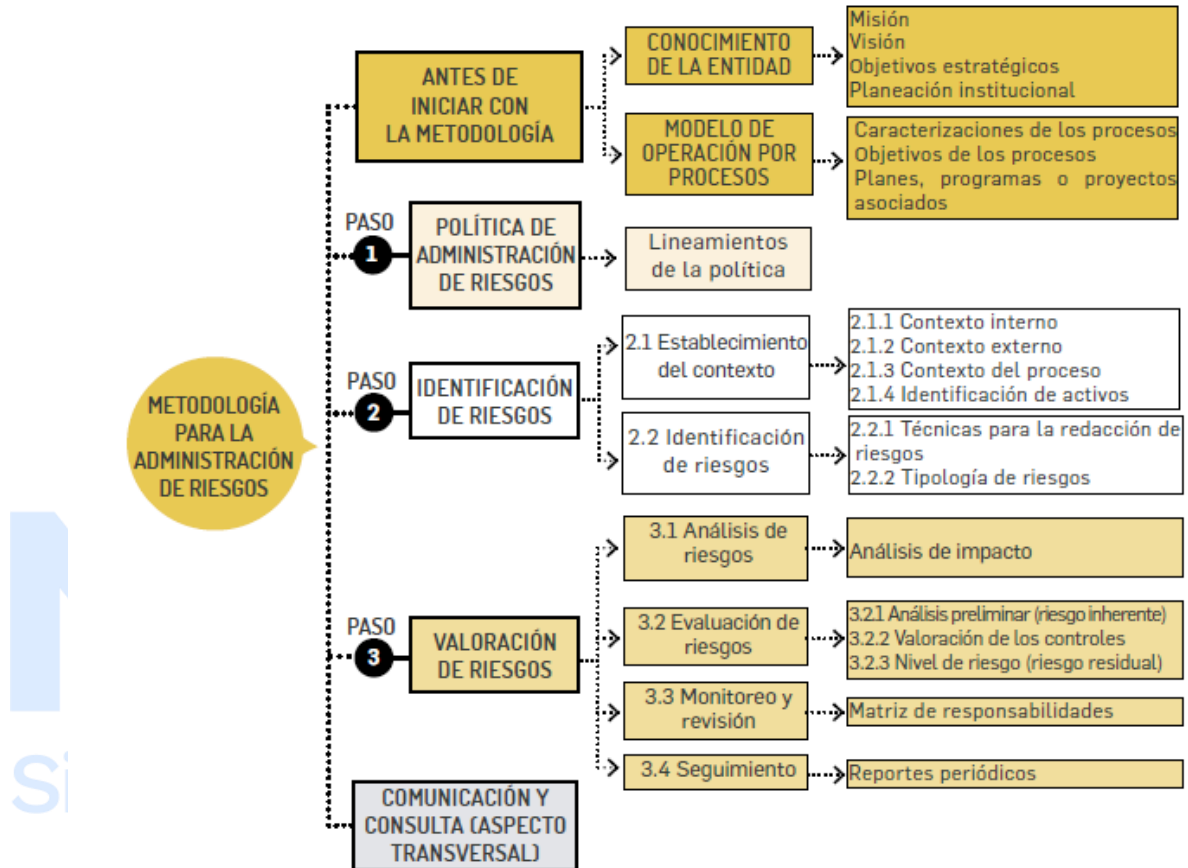



Diagrama 1. Metodología para la Administración del Riesgo. Fuente: Guía Para La Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP. 2018

7.1 POLÍTICA 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 por medio de la cual se identifican y valoran los riesgos por procesos como herramienta estratégica y de gestión que permita anticipar y responder de manera oportuna y óptima 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.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

7.1.1 OBJETIVOS DE LA POLÍTICA

- Controlar a través del Mapa de Riesgos todo el proceso relacionado con el manejo de los riesgos asociados al Sistema Integrado de Gestión.
- 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 el manejo los riesgos de gestión, corrupción, ambientales y seguridad digital.
- 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 digital.
- 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).

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 Y FINANCIEROS: 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 Y CULTURALES: Demografía, responsabilidad social, orden público.
	TECNOLÓGICOS: Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
	LEGALES Y REGLAMENTARIOS: Normatividad externa (leyes, decretos, ordenanzas y acuerdos).

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05


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.
	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 las operaciones.
CONTEXTO DEL PROCESO: Se determinan las características o aspectos esenciales del proceso y sus interrelaciones.	DISEÑO DEL PROCESO: Claridad en la descripción del alcance y objetivo del proceso.
	INTERACCIONES CON OTROS PROCESOS: Relación precisa con otros procesos en cuanto a 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.
	COMUNICACIÓN ENTRE LOS PROCESOS: Efectividad en los flujos de información determinados en la interacción de los procesos.
	ACTIVOS DE SEGURIDAD DIGITAL DEL PROCESO: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano.

Tabla 1. Factores para cada categoría del contexto. Fuente: DAFP. 2018.

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.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

Con el fin de facilitar la identificación de **riesgos de corrupción** y evitar que se confunda con un riesgo de gestión, se debe verificar si cumple con los siguientes criterios.


Descripción del riesgo	Acción u omisión	Uso del poder	Desviar la gestión de lo público	Beneficio privado
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

Tabla 2. Matriz para la definición de riesgos de corrupción. Fuente: Secretaría de Transparencia de la Presidencia de la República.

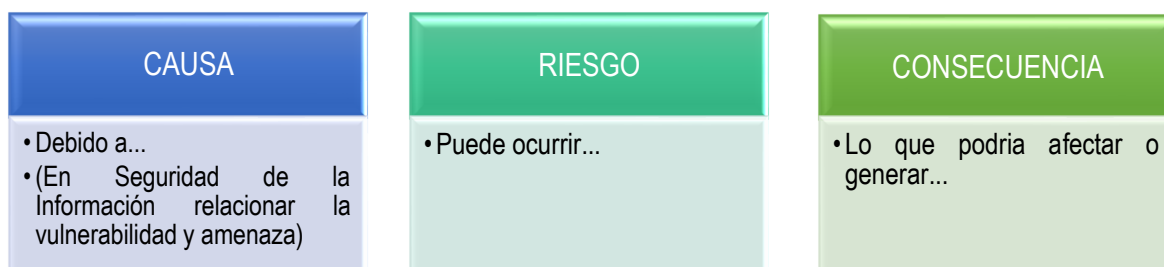
Para identificar **riesgos en seguridad digital** de una manera asertiva es importante verificar posibles hechos que afecten la disponibilidad, integridad o confidencialidad de la información, a nivel físico o lógico, hardware, software y a nivel de instalaciones locativas o legales que lleven a afectar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

Existirían tres (3) tipos de riesgos: pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos. Es también importante identificar las causas que originan el riesgo con 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 y vulnerabilidades comunes se deben consultar en el anexo “Lineamientos para la gestión del riesgo de seguridad digital en entidades públicas” de la Guía Para La Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP.

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.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05


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



En la definición del riesgo se debe evitar iniciar con palabras negativas como: “No...”, “Que no...”, o con palabras que denoten un factor de riesgo (causa) tales como: “ausencia de”, “falta de”, “poco(a)”, “escaso(a)”, “insuficiente”, “deficiente”, “debilidades en...”

Para la identificación de los riesgos y con el objeto de incorporar toda clase de riesgo asociado con el proceso, con la seguridad digital 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 y Diseño de Controles en Entidades Públicas:

- **RIESGO AMBIENTAL:** Posibilidad de que por forma natural o por acción humana se produzca daño en el medio ambiente.
- **RIESGO ESTRATÉGICO:** Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.
- **RIESGOS GERENCIALES:** Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales o la alta dirección.
- **RIESGO DE IMAGEN O REPUTACIONAL:** Posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas.
- **RIESGOS OPERATIVOS:** Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.
- **RIESGOS FINANCIEROS:** Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

- **RIESGOS DE CUMPLIMIENTO:** Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.

- **RIESGOS DE TECNOLOGÍA:** Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.

- **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 SEGURIDAD DIGITAL:** Posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Para la **identificación de los riesgos de corrupción** se deben tener en cuenta algunas actividades susceptibles de riesgos de corrupción identificadas en la Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas del DAFP:

Direccionamiento estratégico (alta dirección).


- Concentración de autoridad o exceso de poder.
- Extralimitación de funciones.
- Ausencia de canales de comunicación.
- Amiguismo y clientelismo.

Financiero (está relacionado con áreas de planeación y presupuesto)

- Inclusión de gastos no autorizados.
- Inversiones de dineros públicos en entidades de dudosa solidez financiera, a cambio de beneficios indebidos para servidores públicos encargados de su administración.
- Inexistencia de registros auxiliares que permitan identificar y controlar los rubros de inversión.
- Inexistencia de archivos contables.
- Afectar rubros que no corresponden con el objeto del gasto en beneficio propio o a cambio de una retribución económica.

De contratación (como proceso o bien los procedimientos ligados a este).

- Estudios previos o de factibilidad deficientes.
- Estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación. (Estableciendo necesidades inexistentes o aspectos que benefician a una firma en particular).

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

- Disposiciones establecidas en los pliegos de condiciones que dirigen los procesos hacia un grupo en particular. (Ej. media geométrica).
- Visitas obligatorias establecidas en el pliego de condiciones que restringen la participación.
- Adendas que cambian condiciones generales del proceso para favorecer a grupos determinados.
- Urgencia manifiesta inexistente.
- Otorgar labores de supervisión a personal sin conocimiento para ello.
- Concentrar las labores de supervisión en poco personal.
- Contratar con compañías de papel que no cuentan con experiencia.

De información y documentación

- Ausencia o debilidad de medidas o políticas de conflictos de interés.
- Concentración de información de determinadas actividades o procesos en una persona.
- Ausencia de sistemas de información.
- Ocultar la información considerada pública para los usuarios.
- Ausencia o debilidad de canales de comunicación
- Incumplimiento de la Ley 1712 de 2014.

De investigación y sanción

- Ausencia o debilidad de canales de comunicación.
- Dilatar el proceso para lograr el vencimiento de términos o la prescripción del mismo.
- Desconocimiento de la ley, mediante interpretaciones subjetivas de las normas vigentes para evitar o postergar su aplicación.
- Exceder las facultades legales en los fallos.


De trámites o servicios internos y externos

- Cobros asociados al trámite.
- Influencia de tramitadores
- Tráfico de influencias: (amiguismo, persona influyente).
- Demorar su realización.

De reconocimiento de un derecho (expedición de licencias o permisos)

- Falta de procedimientos claros para el trámite.
- Imposibilitar el otorgamiento de una licencia o permiso.
- Ofrecer beneficios económicos para aligerar la expedición o para amañar la misma.
- Tráfico de influencias: (amiguismo, persona influyente).

Los **riesgos de seguridad digital** se basan en la afectación de tres criterios en un activo o un grupo de activos dentro del proceso: "Integridad, confidencialidad o disponibilidad"

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

Para el riesgo identificado 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.

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).


7.3.1 ANÁLISIS DEL RIESGO

- Análisis de causas: Los objetivos estratégicos y de proceso se desarrollan a través de actividades, pero no todas tienen la misma importancia, por lo tanto, se debe establecer cuáles de ellas contribuyen mayormente al logro de los objetivos y estas son las actividades críticas o factores claves de éxito; estos factores se deben tener en cuenta al identificar las causas que originan la materialización de los riesgos
- Determinar la 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 número de 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 3. Criterios para calificar la probabilidad.

NIVEL	PROBABILIDAD	DESCRIPCIÓN (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.

Tabla 3. Criterios para calificar la probabilidad. Fuente: DAFP. 2018.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

En caso de que no se cuente con datos históricos sobre el número de eventos que se hayan materializado en un periodo de tiempo, los integrantes del equipo de trabajo deben calificar en privado el nivel de probabilidad en términos de factibilidad, utilizando la siguiente matriz de priorización de probabilidad.

N°	RIESGO	P1	P2	P3	P4	P5	P6	TOT	PROM	
1	Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad	Se espera que el evento ocurra en la mayoría de las circunstancias.	5	4	3	5	3	24	4	4 PROBABLE
2	Otros riesgos identificados	Es viable que el evento ocurra en la mayoría de las circunstancias.								
3	Otros riesgos	El evento podrá ocurrir en algún momento.								

Convenciones:
N.º: número consecutivo del riesgo - P1: participante 1 P... - Tot: total puntaje - Prom.: promedio


Tabla 4. Matriz de priorización de probabilidad. Fuente: DAFP. 2018.

- Determinar nivel de impacto o consecuencias


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

Para la determinación el nivel de impacto o consecuencias de los **riesgos de gestión** se utiliza la Tabla 5. Criterios para calificar el impacto - riesgos de gestión.

NIVELES	IMPACTO (CONSECUENCIAS) CUALITATIVO	IMPACTO (CONSECUENCIAS) CUANTITATIVO
CATASTRÓFICO	<ul style="list-style-type: none"> - 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. 	<ul style="list-style-type: none"> - Impacto que afecte la ejecución presupuestal en un valor $\geq 50\%$. - Pérdida de cobertura en la prestación de los servicios de la entidad $\geq 50\%$. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor $\geq 50\%$. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor $\geq 50\%$ del presupuesto general de la entidad.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

NIVELES	IMPACTO (CONSECUENCIAS) CUALITATIVO	IMPACTO (CONSECUENCIAS) CUANTITATIVO
MAYOR	<ul style="list-style-type: none"> - 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. 	<ul style="list-style-type: none"> - Impacto que afecte la ejecución presupuestal en un valor $\geq 20\%$. - Pérdida de cobertura en la prestación de los servicios de la entidad $\geq 20\%$. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor $\geq 20\%$. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor $\geq 20\%$ del presupuesto general de la entidad.
MODERADO	<ul style="list-style-type: none"> - 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. 	<ul style="list-style-type: none"> - Impacto que afecte la ejecución presupuestal en un valor $\geq 5\%$. - Pérdida de cobertura en la prestación de los servicios de la entidad $\geq 10\%$. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor $\geq 5\%$. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor $\geq 5\%$ del presupuesto general de la entidad.


MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

NIVELES	IMPACTO (CONSECUENCIAS) CUALITATIVO	IMPACTO (CONSECUENCIAS) CUANTITATIVO
MENOR	<ul style="list-style-type: none"> - 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. 	<ul style="list-style-type: none"> - Impacto que afecte la ejecución presupuestal en un valor $\geq 1\%$. - Pérdida de cobertura en la prestación de los servicios de la entidad $\geq 5\%$. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor $\geq 1\%$. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor $\geq 1\%$ del presupuesto general de la entidad.
INSIGNIFICANTE	<ul style="list-style-type: none"> - 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. 	<ul style="list-style-type: none"> - Impacto que afecte la ejecución presupuestal en un valor $\geq 0,5\%$. - Pérdida de cobertura en la prestación de los servicios de la entidad $\geq 1\%$. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor $\geq 0,5\%$. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor $\geq 0,5\%$ del presupuesto general de la entidad.

Tabla 5. Criterios para calificar el impacto - riesgos de gestión. Fuente: DAFP. 2018.


Los criterios para calificar el impacto de los **riesgos de seguridad digital** se encuentran en la Tabla 6. Criterios para calificar el impacto - riesgos de seguridad digital.

NIVEL	VALOR DEL IMPACTO	IMPACTO (CONSECUENCIAS) CUALITATIVO	IMPACTO (CONSECUENCIAS) CUANTITATIVO
INSIGNIFICANTE	1	<ul style="list-style-type: none"> - Afectación $\geq X\%$ de la población. - Afectación $\geq X\%$ del presupuesto anual de la entidad. - No hay afectación medioambiental. 	<ul style="list-style-type: none"> - Sin afectación de la integridad. - Sin afectación de la disponibilidad. - Sin afectación de la confidencialidad.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

NIVEL	VALOR DEL IMPACTO	IMPACTO (CONSECUENCIAS) CUALITATIVO	IMPACTO (CONSECUENCIAS) CUANTITATIVO
MENOR	2	<ul style="list-style-type: none"> - Afectación $\geq X\%$ de la población. - Afectación $\geq X\%$ del presupuesto anual de la entidad. - Afectación leve del medio ambiente requiere de $\geq X$ días de recuperación. 	<ul style="list-style-type: none"> - Afectación leve de la integridad. - Afectación leve de la disponibilidad. - Afectación leve de la confidencialidad.
MODERADO	3	<ul style="list-style-type: none"> - Afectación $\geq X\%$ de la población. - Afectación $\geq X\%$ del presupuesto anual de la entidad. - Afectación leve del medio ambiente requiere de $\geq X$ semanas de recuperación. 	<ul style="list-style-type: none"> - Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. - Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. - Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.
MAYOR	4	<ul style="list-style-type: none"> - Afectación $\geq X\%$ de la población. - Afectación $\geq X\%$ del presupuesto anual de la entidad. - Afectación importante del medio ambiente que requiere de $\geq X$ meses de recuperación. 	<ul style="list-style-type: none"> - Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. - Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. - Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
CATASTRÓFICO	5	<ul style="list-style-type: none"> - Afectación $\geq X\%$ de la población. - Afectación $\geq X\%$ del presupuesto anual de la entidad. - Afectación muy grave del medio ambiente que requiere de $\geq X$ años de recuperación. 	<ul style="list-style-type: none"> - Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. - Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. - Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.

Tabla 6. Criterios para calificar el impacto - riesgos de seguridad digital. Fuente: DAFP.2018


MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

Para la adecuada calificación de riesgos de seguridad digital se debe tener en cuenta lo siguiente:

- Las variables confidencialidad, integridad y disponibilidad se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital (GD) del Ministerio de Tecnologías de la Información y las Comunicaciones.
- La variable población se define teniendo en cuenta el establecimiento del contexto externo de la entidad, es decir, que la consideración de población va a estar asociada a las personas a las cuales se les prestan servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectadas por la materialización de algún riesgo en los activos identificados.
Los porcentajes en las escalas pueden variar, según la entidad y su contexto.
- La variable presupuesta es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.
- La variable ambiental estará también alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizada en la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existir afectación ambiental.

Para la determinación el nivel de impacto o consecuencias de los **riesgos de corrupción** se utiliza la Tabla 7. Criterios para calificar el impacto - 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		

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

FORMATO PARA DETERMINAR EL IMPACTO		
No	PREGUNTA	RESPUESTA
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	
19	Generar daño ambiental	


Tabla 7. Criterios para calificar el impacto - riesgos de corrupción. Fuente: DAFP. 2018.

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:

NIVEL	IMPACTO	DESCRIPCIÓN	RIESGOS DE CORRUPCIÓN
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 preguntas(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 DIECINUEVE preguntas genera un impacto CATASTRÓFICO

Tabla 6. Criterios para calificar el impacto - riesgos de corrupción. Fuente: DAFP.2018

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

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

- Estimar el nivel del riesgo inicial

Se logra a través de la determinación de la probabilidad y el impacto como se mencionó anteriormente por medio de las tablas establecidas. Para su determinación se utiliza la Matriz de criticidad de 5x5, la cual determina que para ubicar el nivel de riesgo se cuenta con cinco niveles en probabilidad y 5 niveles en impacto.

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

Al momento de definir las actividades de control por parte de la primera línea de defensa, es importante considerar que los controles estén bien diseñados, es decir, que efectivamente estos mitigan las causas que hacen que el riesgo se materialice.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05


- Valoración de los controles – diseño de controles

Las actividades de control, independientemente de la tipología de riesgo a tratar, deben tener una adecuada combinación para prevenir que la situación de riesgo se origine. Ahora, en caso de que la situación de riesgos se presente, esta debe ser detectada de manera oportuna, es así, como se encuentra la siguiente clasificación de las actividades de control:

- **Controles preventivos:** Controles que están diseñados para evitar un evento no deseado en el momento en que se produce. Este tipo de controles intentan evitar la ocurrencia de los riesgos que puedan afectar el cumplimiento de los objetivos.
- **Controles detectivos:** Controles que están diseñados para identificar un evento o resultado no previsto después de que se haya producido. Buscan detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes.

Al momento de definir si un control o los controles mitigan de manera adecuada el riesgo se deben considerar, desde la redacción del mismo, las siguientes variables:

- Paso 1: Debe tener definido el responsable de llevar a cabo la actividad de control. Persona asignada para ejecutar el control. Debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso y sus responsabilidades deben ser adecuadamente segregadas o redistribuidas entre diferentes individuos, para reducir así el riesgo de error o de actuaciones irregulares o fraudulentas. Si ese responsable quisiera hacer algo indebido, por sí solo, no lo podría hacer. Si la respuesta es que cumple con esto, quiere decir que el control está bien diseñado, si la respuesta es que no cumple, tenemos que identificar la situación y mejorar el diseño del control con relación a la persona responsable de su ejecución.
- Paso 2: Debe tener una periodicidad definida para su ejecución. El control debe tener una periodicidad específica para su realización (diario, mensual, trimestral, anual, etc.) y su ejecución debe ser consistente y oportuna para la mitigación del riesgo. Por lo que en la periodicidad se debe evaluar si este previene o se detecta de manera oportuna el riesgo. Una vez definido el paso 1 - responsable del control, debe establecerse la periodicidad de su ejecución.
Cada vez que se releva un control debemos preguntarnos si la periodicidad en que este se ejecuta ayuda a prevenir o detectar el riesgo de manera oportuna. Si la respuesta es SÍ, entonces la periodicidad del control está bien diseñada.
- Paso 3: Debe indicar cuál es el propósito del control. El control debe tener un propósito que indique para qué se realiza, y que ese propósito conlleve a prevenir las causas que generan el riesgo (verificar, validar, conciliar, comparar, revisar, cotejar) o detectar la materialización del riesgo, con el objetivo de llevar a cabo los ajustes y correctivos en el diseño del control o en su ejecución. El solo hecho de establecer un procedimiento o contar con una política por sí sola, no va a prevenir o detectar la


MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

materialización del riesgo o una de sus causas. Siguiendo las variables a considerar en la evaluación del diseño de control revisadas, veamos algunos ejemplos de cómo se deben redactar los controles, incluyendo el propósito del control, es decir, lo que este busca.

- Paso 4: Debe establecer el cómo se realiza la actividad de control. El control debe indicar el cómo se realiza, de tal forma que se pueda evaluar si la fuente u origen de la información que sirve para ejecutar el control, es confiable para la mitigación del riesgo. Cuando estemos evaluando el control debemos preguntarnos si la fuente de información utilizada es confiable.
- Paso 5: Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control. El control debe indicar qué pasa con las observaciones o desviaciones como resultado de ejecutar el control. Al momento de evaluar si un control está bien diseñado para mitigar el riesgo, si como resultado de un control preventivo se observan diferencias o aspectos que no se cumplen, la actividad no debería continuarse hasta que se subsane la situación o si es un control que detecta una posible materialización de un riesgo, deberían gestionarse de manera oportuna los correctivos o aclaraciones a las diferencias presentadas u observaciones.
- Paso 6: Debe dejar evidencia de la ejecución del control. El control debe dejar evidencia de su ejecución. Esta evidencia ayuda a que se pueda revisar la misma información por parte de un tercero y llegue a la misma conclusión de quien ejecutó el control y se pueda evaluar que el control realmente fue ejecutado de acuerdo con los parámetros establecidos y descritos anteriormente.

Partiendo de lo anterior, en el momento de realizar el análisis y evaluación del diseño del control se deben tener en cuenta las variables mostradas por medio de la Tabla 9. Peso o participación de cada variable en el diseño del control.

CRITERIO DE EVALUACIÓN	OPCIÓN DE RESPUESTA AL CRITERIO DE EVALUACIÓN	PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
Asignación del responsable	Asignado	15
	No Asignado	0
Segregación y autoridad del responsable	Adecuado	15
	Inadecuado	0
Periodicidad	Oportuna	15
	Inoportuna	0
Propósito	Prevenir	15
	Detectar	10
	No es un control	0
Cómo se realiza la actividad de control	Confiable	15
	No confiable	0

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

CRITERIO DE EVALUACIÓN	OPCIÓN DE RESPUESTA AL CRITERIO DE EVALUACIÓN	PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
Qué pasa con las observaciones o desviaciones	Se investigan y resuelven oportunamente	15
	No se investigan y resuelven oportunamente	0
Evidencia de la ejecución del control	Completa	10
	Incompleta	5
	No existe	0

Tabla 7. Peso o participación de cada variable en el diseño del control. Fuente: DAFP.2018

Una vez calificado el diseño del control se debe establecer la evaluación de acuerdo con la siguiente tabla:

RANGO DE CALIFICACIÓN DEL DISEÑO	RESULTADO – PESO EN LA EVALUACION DEL DISEÑO DEL CONTROL
Fuerte	Calificación entre 96 y 100
Moderado	Calificación entre 86 y 95
Débil	Calificación entre 0 y 85

Tabla 80. Tabla de Evaluación del Diseño del Control. Fuente: DAFP. 2018.


Si el resultado de las calificaciones del control, o el promedio en el diseño de los controles, está por debajo de 96%, se debe establecer un plan de acción que permita tener un control o controles bien diseñados.

Teniendo en cuenta que el solo diseño del control no es garantía de la acción del mismo frente a la prevención o mitigación de la materialización del riesgo se debe evaluar si el control se ejecuta de acuerdo con la siguiente calificación:

RANGO DE CALIFICACIÓN DE LA EJECUCIÓN	RESULTADO – PESO DE LA EJECUCIÓN DEL CONTROL
Fuerte	El control se ejecuta de manera consistente por parte del responsable.
Moderado	El control se ejecuta algunas veces por parte del responsable.
Débil	El control no se ejecuta por parte del responsable.

Tabla 91. Tabla de Evaluación de la Ejecución del Control. Fuente: DAFP.2018.

Por último, se debe realizar la calificación de la solidez del control teniendo en cuenta los resultados de la calificación del diseño del control y de la ejecución del mismo, la calificación de la solidez de cada control asumirá la calificación del diseño o ejecución con menor calificación entre fuerte, moderado y débil. tal como se detalla en la siguiente tabla:

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

PESO DEL DISEÑO DE CADA CONTROL	PESO DE LA EJECUCIÓN DE CADA CONTROL	SOLIDEZ INDIVIDUAL DE CADA CONTROL: FUERTE: 100 MODERADO 50 DEBIL 0	DEBE ESTABLECER ACCIONES PARA FORTALECER EL CONTROL SÍ / NO
Fuerte: calificación entre 96 y 100	fuerte (siempre se ejecuta)	fuerte + fuerte = fuerte	No
	moderado (algunas veces)	fuerte + moderado = moderado	Sí
	débil (no se ejecuta)	fuerte + débil = débil	Sí
Moderado: calificación entre 86 y 95	fuerte (siempre se ejecuta)	moderado + fuerte = moderado	Sí
	moderado (algunas veces)	moderado + moderado = moderado	Sí
	débil (no se ejecuta)	moderado + débil = débil	Sí
Débil: calificación entre 0 y 85	fuerte (siempre se ejecuta)	débil + fuerte = débil	Sí
	moderado (algunas veces)	débil + moderado = débil	Sí
	débil (no se ejecuta)	débil + débil = débil	Sí

Tabla 102. Tabla de Evaluación de la Solidez del Control. Fuente: DAFP.2018.


- Nivel de riesgo residual

Para determinar los riesgos residuales se debe evaluar el impacto de todos los controles diseñados por cada riesgo, por lo que hay que consolidar el conjunto de los controles asociados a las causas, para evaluar si estos de manera individual y en conjunto sí ayudan al tratamiento de los riesgos. La solidez del conjunto de controles se obtiene calculando el promedio aritmético simple de los controles por cada riesgo.

CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES	
Fuerte	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100.
Moderado	El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre 50 y 99.
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50.

Tabla 113. Tabla de calificación de la solidez del conjunto de controles. Fuente: DAFP.2018.

Una vez terminado de calificar el conjunto de controles para cada riesgo, se debe establecer el desplazamiento de un riesgo inherente en su probabilidad o impacto para el cálculo del riesgo residual lo cual se realizará de acuerdo con la siguiente tabla:

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

SOLIDEZ DEL CONJUNTO DE CONTROLES	CONTROLES AYUDAN A DISMINUIR LA PROBABILIDAD	CONTROLES AYUDAN A DISMINUIR EL IMPACTO	# COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPLAZA EN EL EJE DE PROBABILIDAD	# COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPLAZA EN EL EJE DE IMPACTO
Fuerte	Directamente	Directamente	2	2
Fuerte	Directamente	Indirectamente	2	1
Fuerte	Directamente	No disminuye	2	0
Fuerte	No disminuye	Directamente	0	2
Moderado	Directamente	Directamente	1	1
Moderado	Directamente	Indirectamente	1	0
Moderado	Directamente	No disminuye	1	0
Moderado	No disminuye	Directamente	0	1

Tabla 124. Resultados de los posibles desplazamientos de la probabilidad y del impacto de los riesgos.
Fuente: DAFP.2018.


7.3.3 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):** Se abandonan las actividades que dan lugar al riesgo y se decide no iniciar o no continuar con las actividades que lo causan.
- **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.

Para mitigar/tratar los riesgos de seguridad digital se deben emplear como mínimo los controles del anexo A de la ISO/IEC 27001:2013.

- **Compartir o transferir el riesgo (TR):** Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. 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.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

- **Aceptar 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. Pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y por ende se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

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.

7.4 MONITOREO Y REVISIÓN

El monitoreo y revisión tiene como propósito valorar la efectividad de los controles establecidos por la entidad, el nivel de ejecución de los planes de manejo o tratamiento de los riesgos que permiten asegurar los resultados de la gestión, así como detectar las desviaciones y tendencias para generar recomendaciones sobre el mejoramiento de los procesos, y determinar si existen cambios en el contexto interno o externo, incluyendo los cambios en los criterios de riesgo y en el propio riesgo.

RESPONSABLES DE LOS PROCESOS

El monitoreo y revisión de la gestión de riesgos, está alineada con la dimensión de MIPG de Control Interno, que se desarrolla con el MECI a través de un esquema de asignación de responsabilidades y roles, el cual se distribuye en diversos servidores de la entidad en el marco de las líneas de defensa así (Fuente: Manual MIPG)


LINEA ESTRATEGICA: Define el marco general para la gestión del riesgo y el control

1ERA LINEA DE DEFENSA: La gestión operacional se encarga del mantenimiento efectivo de controles internos, ejecutar procedimientos de riesgo y el control sobre una base del día a día. La gestión operacional identifica, evalúa, controla y mitiga los riesgos.

De acuerdo a lo anterior, cada líder de proceso debe mantener la traza o documentación respectiva de todas las actividades realizadas que garanticen de forma razonable que dichos riesgos no se materializarán y por ende que los objetivos del proceso se cumplan.

2DA LINEA: Asegura que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente

3RA LINEA DE DEFENSA (Oficina de Control Interno): Proporciona Información sobre la efectividad del SCI., la operación de la 1ª y 2ª Línea de defensa con un enfoque basado en riesgos

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUÍA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

Por ende, de acuerdo a su rol de evaluación del riesgo, mediante los ejercicios auditores, dicha oficina analizará el diseño e idoneidad de los controles, determinando si son o no adecuados para prevenir o mitigar los riesgos de los procesos, de acuerdo a su comportamiento, estableciendo la efectividad de los mismos.

Las Líneas de Defensa en el Modelo Estándar de Control Interno

Línea Estratégica



- Define el marco general para la gestión del riesgo y el control a cargo de la **Alta Dirección y el Comité Institucional de Coordinación de Control Interno**.
- Este nivel analiza los riesgos y amenazas institucionales al cumplimiento de los planes estratégicos (objetivos, metas, indicadores).
- Define el marco general para la gestión del riesgo (política de administración del riesgo) y garantiza el cumplimiento de los planes de la Entidad.
- G-E-SIG-05 "Guía Metodológica para Identificación y Valoración Riesgos por Procesos del MADS" adoptada en el Comité Institucional de Coordinación de Control Interno, el 10 de julio de 2019.



1ª Línea de defensa



- A cargo de los **Jefes de área o líderes de proceso, facilitadores y sus equipos de trabajo**.
- Se encarga del mantenimiento efectivo de los controles internos, implementar la G-E-SIG-05 "Guía Metodológica para Identificación y Valoración Riesgos por Procesos del MADS" y los controles establecidos en el mapa y plan de manejo de riesgos.
- Son responsables de implementar acciones correctivas e igualmente detecta las deficiencias del control.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	MADSIG Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

2ª Línea de defensa

- La **Oficina Asesora de Planeación con apoyo de los facilitadores de los procesos** realizan el monitoreo y evaluación del estado de los controles y la gestión del riesgo. Entre ellos pueden citarse jefes de planeación a través del grupo SIG, coordinadores de equipos de trabajo, supervisores de contratos, Comité de contratación, áreas financieras, de TIC, entre otros, que generen información para el aseguramiento de la operación.
- Asegura que los controles y procesos de gestión del riesgo de la 1ª Línea de defensa sean apropiados y funcionen correctamente.
- Ejerce el control y la gestión de riesgos, las funciones de cumplimiento, seguridad y calidad.
- Supervisa la implementación de prácticas de gestión de riesgo eficaces por parte de la primera línea y ayuda a los responsables de riesgos a distribuir información adecuada sobre riesgos a todos los servidores del Ministerio.



M
Sistema


G
ción

3ª Línea de defensa

- A cargo de la **Oficina de Control Interno del Ministerio**.
- Proporciona información sobre la efectividad del Sistema de Control Interno, la operación de la primera y segunda línea de defensa con un enfoque basado en riesgos.
- La función de auditoría interna, a través de un enfoque basado en el riesgo, proporciona aseguramiento sobre la eficacia institucional, gestión de riesgos y control interno a la Alta Dirección, incluyendo el funcionamiento de la primera y segunda línea de defensa.



Diagrama 2. Las líneas de defensa en el Modelo Estándar de Control Interno Fuente: Adaptado de declaración de posición. Las tres líneas de defensa para una efectiva gestión de riesgo y control. Instituto Internacional de auditores IIA 2013.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUÍA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

De otra parte y en concordancia con “La Guía para la Gestión del riesgo de Corrupción” de la Presidencia de la Republica, se realizaran seguimientos periódicos sobre los posibles actos de corrupción mediante la evaluación de los riesgos de corrupción, equiparando dicho seguimiento a las fechas establecidas de seguimiento al Plan Anticorrupción y atención al ciudadano, las cuales son 3 veces al año empezando el 1ero con corte al 30 de abril, el 2do con corte al 31 de agosto y el 3ero con corte al 31 de diciembre.

Dicho seguimiento se publicará en la página web de la entidad o en lugar de fácil acceso al ciudadano.

7.5 MAPA DE RIESGOS INSTITUCIONAL

El mapa de riesgos institucional del Ministerio de Ambiente y Desarrollo Sostenible se publicará en la página web de la entidad en el link <https://www.minambiente.gov.co/index.php/component/content/article?id=5&Itemid=516>, una vez sea aprobado por los responsables de los procesos en el Comité Institucional de Gestión y Desempeño.

Se realiza el diligenciamiento del formato F-E-SIG-28 “Mapa de riesgos institucional” que contiene el registro de los riesgos identificados, establece la clase de riesgo, identifica las causas, las consecuencias, así como, la probabilidad e impacto, evaluando el riesgo inherente.

Posteriormente, se realiza el análisis de las estrategias que contrarresten las causas raíz, incluyendo las actividades de control, valorando los controles para determinar el riesgo residual y con base en su contenido se establece la opción de tratamiento a la que corresponden.


Mediante la definición del plan de manejo del riesgo se relaciona el soporte o indicador con el que se evidenciará el cumplimiento de cada actividad, el responsable de adelantarla (relacionando el cargo) y el tiempo específico para su cumplimiento.

Al final de todas las actividades de control establecidas en el plan de manejo del riesgo para atacar las causas del mismo, se debe relacionar el plan de contingencia a implementar una vez el riesgo se materialice, teniendo en cuenta que este tipo de acciones son de aplicación inmediata y a corto plazo para restablecer, cuanto antes, la normalidad de las actividades para el logro de los objetivos del proceso.

Por último, se evidencia el monitoreo y seguimiento frente a las responsabilidades de la 1era, 2da y 3era línea de defensa en el marco del proceso de administración del riesgo

8 COMUNICACIÓN Y CONSULTA

La comunicación y la consulta deberán surtir 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.

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	GUIA DE ADMINISTRACIÓN DEL RIESGO	 Sistema Integrado de Gestión
	Proceso: Administración del Sistema Integrado de Gestión	
Versión: 4	Vigencia: 31/07/2020	Código: G-E- SIG-05

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.

