MANUAL DE ADMINISTRACIÓN DEL RIESGO

MANUAL DE ADMINISTRACIÓN DE RIESGOS

La administración del riesgo tiene una gran importancia, dado el dinamismo y los constantes cambios que se presentan en un mundo globalizado. Estos cambios hacen que las entidades deban enfrentarse a factores tanto internos como externos que pueden crear incertidumbre sobre el cumplimiento de sus objetivos. Es así, como el efecto que dicha incertidumbre tiene en los objetivos de una organización se denomina riesgo.

En este sentido, INFOTEP, ve la necesidad de actualizar el manual de administración de riesgos teniendo en cuenta los lineamientos establecidos en el Modelo Integrado de Planeación y Gestión – MIPG, el Modelo Estándar de Control Interno MECI, la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4, y la política de administración del riesgo, herramientas que en su conjunto le permiten realizar una correcta administración de los riesgos presentes en sus procesos, le permite ser más eficiente y eficaz en el cumplimiento de sus objetivos. INFOTEP elabora este Manual de Administración de Riesgos, con el objetivo de tener las políticas y procedimientos claros para la implementación de esta temática.

1. MARCO NORMATIVO

NORMA	DESCRIPCIÓN
Ley 87 de 1993	Por la cual se establecen normas para el ejercicio del control interno en las
	entidades y organismos del Estado y se dictan otras disposiciones.
	(Modificada parcialmente por la Ley 1474 de 2011). *Artículo 2 Objetivos del control*
	interno: literal a). Proteger los recursos de la organización, buscando su adecuada
	administración ante posibles riesgos que los afectan. Literal f). Definir y aplicar
	medidas para prevenir los riesgos, detectar y corregir las desviaciones que se
	presenten en la organización y que puedan afectar el logro de los objetivos.
Ley 489 de 1998	Estatuto Básico de Organización y Funcionamiento de la Administración Pública.
	Capítulo VI. Sistema Nacional de Control Interno
Decreto 2145 de 1999	Por el cual se dictan normas sobre el Sistema Nacional de Control Interno de las
	Entidades y Organismos de la Administración Pública del orden nacional y
	territorial y se dictan otras disposiciones.
	(Modificado parcialmente por el Decreto 2593 del 2000 y por el Art. 8º. de la ley

	1474 de 2011)
Directiva presidencial 09 de 1999	Lineamientos para la implementación de la política de lucha contra la corrupción.
Decreto 2593 del 2000	Por el cual se modifica parcialmente el Decreto 2145 de noviembre 4 de 1999.
Decreto 1537 de 2001	Por el cual se reglamenta parcialmente la Ley 87 de 1993 en cuanto a elementos
	técnicos y administrativos que fortalezcan el sistema de control interno de las
	entidades y organismos del Estado.
	El parágrafo del Artículo 4º señala los objetivos del sistema de control interno (…)
	define y aplica medidas para prevenir los riesgos, detectar y corregir las
	desviaciones (…) y en su Artículo 3º establece el rol que deben desempeñar las
	oficinas de control interno (…) que se enmarca en cinco tópicos (…) valoración de
	riesgos. Así mismo establece en su Artículo 4º la administración de riesgos, como
	parte integral del fortalecimiento de los sistemas de control interno en las
	entidades públicas (…).
Decreto 1599 de 2005	Por el cual se adopta el Modelo Estándar de Control Interno para el Estado
	colombiano y se presenta el anexo técnico del MECI 1000:2005. 1.3 Componentes
	de administración del riesgo.
Decreto 943 de 2014	Por el cual se actualiza el Modelo Estándar de Control Interno (MECI).
Decreto 4485 de 2009	Por el cual se adopta la actualización de la NTCGP a su versión 2009.
	Numeral 4.1 Requisitos generales literal g) "establecer controles sobre los riesgos
	identificados y valorados que puedan afectar la satisfacción del cliente y el logro
	de los objetivos de la entidad; cuando un riesgo se materializa es necesario tomar
	acciones correctivas para evitar o disminuir la probabilidad de que vuelva a
	suceder". Este decreto aclara la importancia de la Administración del riesgo en el
	Sistema de Gestión de la Calidad en las entidades.
Ley 1474 de 2011	Estatuto Anticorrupción. Artículo 73. "Plan Anticorrupción y de Atención al
	Ciudadano" que deben elaborar anualmente todas las entidades,
	incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar
	esos riesgos, las estrategias anti-trámites y los mecanismos para mejorar la
	atención al ciudadano.
Decreto 4637 de 2011	Crea la Secretaría de Transparencia en el Departamento Administrativo de la
	Presidencia de la República, quien establece lineamientos para la prevención de
	la corrupción.
Decreto 1649 de 2014	Funciones de la Secretaría de Transparencia: 13) Señalar la metodología para
	diseñar y hacer seguimiento a las estrategias de lucha contra la corrupción y de
	atención al ciudadano que deberán elaborar anualmente las entidades del orden
	nacional y territorial.
Decreto 1081 de 2015	Señala como metodología para elaborar la estrategia de lucha contra la corrupción
	la contenida en el documento "Estrategias para la construcción del Plan
	Anticorrupción y de Atención al Ciudadano."
Decreto 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único
	Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de

2. MARCO CONCEPTUAL

El Modelo Integrado de Planeación y Gestión MIPG es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio, según dispone el Decreto 1499 de 2017.

MIPG busca mejorar la capacidad del Estado para cumplirle a la ciudadanía, incrementando la confianza de la ciudadanía en sus entidades y en los servidores públicos, logrando mejores niveles de gobernabilidad y legitimidad del aparato público y generando resultados con valores a partir de una mejor coordinación interinstitucional, compromiso del servidor público, mayor presencia en el territorio y mejor aprovechamiento y difusión de información confiable y oportuna es una de los objetivos de la puesta en marcha del Modelo Integrado de Planeación y Gestión MIPG.

Para INFOTEP la administración de riesgos es una herramienta fundamental que permite asegurar el cumplimiento de su misión institucional y el desarrollo de sus actividades mediante el cumplimiento de los objetivos trazados dentro del Plan Institucional.

Por lo anterior, se definen los criterios orientadores respecto al tratamiento de los riesgos, a fin de mitigar sus efectos en la institución siendo éste, el objetivo de este manual que expone la metodología a seguir para identificar, valorar y evaluar los riesgos en la entidad, es decir la manera de abordar la administración de los riesgos institucionales, socializar con todos los funcionarios un lenguaje común sobre el tema y difundir los lineamientos que permitan la sostenibilidad de la administración del riesgo.

3. CONCEPTOS

- **Aceptación del riesgo**: Decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.
- **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 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. Se constituye en el componente de control que al interactuar con sus diferentes elementos le permite a la entidad pública, autocontrolar aquellos eventos que pueden afectar el cumplimiento de sus objetivos.
- **Amenazas**: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Análisis de riesgo**: Elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad para su aceptación y manejo. Se debe llevar a cabo un uso sistemático de la información disponible para determinar qué tan frecuentemente pueden ocurrir eventos especificados y la magnitud de sus consecuencias.
- **Apetito al riesgo**: magnitud y tipo de riesgo que la entidad está dispuesta a buscar o retener.
- **Causa**: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Compartir el riesgo**: Se asocia con la forma de protección para disminuir las pérdidas que ocurran luego de la materialización de un riesgo, es posible realizarlo mediante contratos, seguros, cláusulas contractuales u otros medios que puedan aplicarse
- **Confidencialidad**: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

- **Consecuencia**: son 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.
- **Control**: medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).
- **Control detectivo**: 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.
- **Control preventivo**: 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.
- **Disponibilidad**: propiedad de ser accesible y utilizable a demanda por una entidad.
- **Factores de riesgo**: Manifestaciones o características medibles u observables de un proceso que indican la presencia de riesgos o tienden a aumentar la exposición, pueden ser internos o externos de la entidad.
- **Gestión del riesgo**: 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 del riesgo**: 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. Se puede entender como el proceso que permite determinar qué podría suceder, por qué sucedería y de qué manera se llevaría a cabo.
- **Impacto**: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Integridad**: propiedad de exactitud y completitud.
- **Mapa de riesgos**: documento con la información resultante de la gestión del riesgo.
- **Nivel de aceptación del riesgo**: son los criterios de aceptación de riesgos establecidos que se emplean durante la etapa de evaluación de riesgos.
- **Plan Anticorrupción y de Atención al Ciudadano**: plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

- **Probabilidad**: se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.
- **Riesgo**: es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. 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.
- **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.
- **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 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.
- **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.
- **Riesgos estratégicos**: 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 y/o la alta dirección.
- **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.
- **Riesgo inherente**: es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
- **Riesgos tecnológicos**: posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.
- **Riesgos operativos**: posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.

- **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.
- **Tratamiento del riesgo**: consiste en seleccionar y aplicar las medidas más adecuadas, con el fin de poder modificar el riesgo, para evitar de este modo los daños intrínsecos al factor de riesgo, o bien aprovechar las ventajas que pueda reportarnos.
- **Valoración del riesgo**: Busca identificar y analizar los riesgos que enfrenta la entidad, tanto de fuentes internas como externas relevantes para la consecución de los objetivos, para administrarlos.
- **Vulnerabilidad**: es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

4. POLÍTICA

Establecer el marco general para la administración de los riesgos en INFOTEP mediante la ejecución de un proceso metódico y continuo que contribuya al mejoramiento constante de las actividades y al cumplimiento de los objetivos de la Entidad.

5. METODOLOGIA

Análisis y calificación de los Riesgos

5.1. Análisis de la Probabilidad

La probabilidad es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos de la entidad, pudiendo entorpecer el desarrollo de sus funciones. La forma de medir su probabilidad y ocurrencia para los distintos tipos de riesgos (gestión, corrupción y seguridad digital), es la siguiente:

Probabilidad

NIVEL	DESCRIPTOR	DESCRIPCIÓN	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.

5.2. Análisis de Impacto

Por impacto se entienden las consecuencias que puede ocasionar a la entidad la materialización del riesgo. De acuerdo con el tipo de riesgo, el impacto se calcula de manera diferente, así:

Criterios para calificar el impacto para riesgos de gestión

NIVEL	IMPACTO	CONSECUENCIAS CUANTITATIVAS	CONSECUENCIAS CUALITATIVAS
1	Insignificante	• Impacto que afecte la ejecución presupuestal en un valor ≥0,5% • Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%. • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5% • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la entidad	• No hay interrupción de las operaciones de la entidad. • No se generan sanciones económicas o administrativas. • No se afecta la imagen institucional de forma significativa
2	Menor	• Impacto que afecte la ejecución presupuestal en un valor ≥1% • Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%. • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥1%	• 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.

		• Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la entidad.	
3	Moderado	• Impacto que afecte la ejecución presupuestal en un valor ≥5% • Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5% • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad	• Interrupción de las operaciones de la Entidad por un día. • Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. • Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. • Reproceso de actividades y aumento de carga operativa. • Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. • Investigaciones penales, fiscales o disciplinarias
4	Mayor	• Impacto que afecte la ejecución presupuestal en un valor ≥20% • Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20% • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la Comisión	• 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.
5	Catastrófico	• Impacto que afecte la ejecución presupuestal en un valor ≥50% • Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50% • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la Entidad	• Interrupción de las operaciones de la Entidad por más de cinco (5) días. • Intervención por parte de un ente de control u otro ente regulador. • Pérdida de Información crítica para la entidad que no se puede recuperar. • Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. • Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.

Criterios para calificar el impacto para riesgos de seguridad digital

NIVEL	IMPACTO	CONSECUENCIAS CUANTITATIVAS	CONSECUENCIAS CUALITATIVAS

1	Insignificante	• Afectación ≥1% de la población. • Afectación ≥0,5% del presupuesto anual de la entidad.	• Sin afectación de la integridad. • Sin afectación de la disponibilidad. • Sin afectación de la confidencialidad.
2	Menor	• Afectación ≥5% de la población. • Afectación ≥1% del presupuesto anual de la entidad.	• Afectación leve de la integridad. • Afectación leve de la disponibilidad. • Afectación leve de la confidencialidad.
3	Moderado	• Afectación ≥10% de la población. • Afectación ≥5% del presupuesto anual de la entidad.	• Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. • Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. • Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.
4	Mayor	• Afectación ≥20% de la población. • Afectación ≥20% del presupuesto anual de la entidad.	• Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. • Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. • Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
5	Catastrófico	• Afectación ≥50% de la población. • Afectación ≥50% del presupuesto anual de la entidad.	• 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

Criterios para calificar el impacto para riesgos de corrupción

Para calificar el impacto de los riesgos de corrupción, se debe dar respuesta a las siguientes preguntas:

Pregunta. 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 misión de la entidad?		
4 ¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5 ¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6 ¿Generar pérdida de recursos económicos?		
7 ¿Afectar la generación de los productos o la prestación de servicios?		
¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9 ¿Generar pérdida de información de la entidad?		
10 ¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11 ¿Dar lugar a procesos sancionatorios?		
12 ¿Dar lugar a procesos disciplinarios?		
13 ¿Dar lugar a procesos fiscales?		
14 ¿Dar lugar a procesos penales?		
15 ¿Generar pérdida de credibilidad del sector?		
16 ¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17 ¿Afectar la imagen regional?		
18 ¿Afectar la imagen nacional?		
19 ¿Generar daño ambiental?		

La calificación de impacto de riesgos de corrupción no tiene los niveles de insignificante y menor, y se califica de la siguiente manera:

Nivel	Calificación	Consecuencia
MODERADO	Responder afirmativamente de UNA a CINCO preguntas genera un impacto moderado.	Genera medianas consecuencias sobre la entidad
MAYOR	Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor.	Genera altas consecuencias sobre la entidad.
CATASTRÓFICO	Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.	Genera consecuencias desastrosas para la entidad

1. Niveles de tratamiento de los riesgos y mapa de calor

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

Aceptar el riesgo: significa que no se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. Ningún riesgo de corrupción puede tener como tratamiento, el aceptar el riesgo.

Reducir el riesgo: se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos. Por lo general conlleva a la implementación de controles.

Evitar el riesgo: se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que lo provoca.

Compartir el riesgo: se reduce la probabilidad o el impacto del riesgo, transfiriendo o compartiendo una parte del riesgo. Para el caso de los riesgos de corrupción, se puede compartir, pero no se puede transferir su responsabilidad.

De acuerdo con lo anterior, se establecen a continuación los niveles de tratamiento a los riesgos:

Nivel BAJO: se ACEPTARÁ el riesgo y administrará por medio de las actividades propias del proceso asociado y su control y registro de avance se realizará semestralmente por medio del informe de desempeño.

Nivel MEDIO O MODERADO: se deberá incluir este riesgo en el Mapa de riesgos Institucional, se establecerán acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo, se administrarán mediante seguimiento trimestral y se registrarán sus avances en los informes de desempeño.

Nivel ALTO: se deberá incluir el riesgo en el Mapa de riesgos Institucional y se establecerán acciones de control preventivas que permitan EVITAR o COMPARTIR la materialización del riesgo. La administración de estos riesgos será con periodicidad trimestral y su adecuado control se registrará en los informes de desempeño.

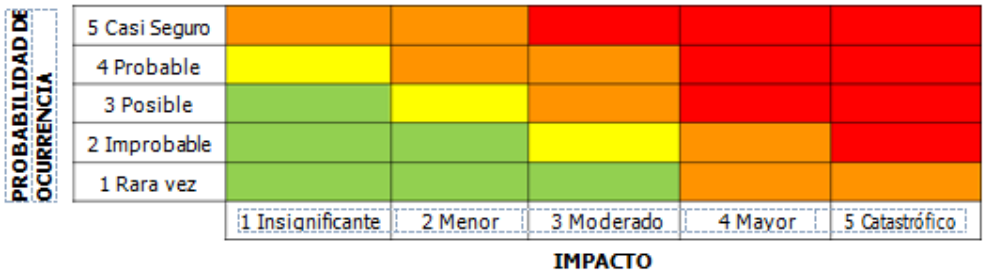
Nivel EXTREMO o CATASTRÓFICO: Si bien el primer llamado es a abandonar la actividad que genera el riesgo, INFOTEP no considera prudente, por ahora eliminar actividades dado que las mismas pueden generar el no cumplimiento de su misión, por lo que se incluirá el riesgo en el Mapa de riesgos Institucional, se establecerán acciones de control preventivas y correctivas que permitan EVITAR o COMPARTIR la materialización del riesgo. La administración de estos riesgos será con periodicidad mensual y su adecuado control se registrará en informes presentados a la Alta Dirección.

Adicionalmente, se deberán documentar al interior de los procesos planes preventivos (antes de que ocurra el evento) y contingencia (después de que ocurra el evento) para tratar el riesgo materializado, con criterios de oportunidad, evitando el menor daño en la prestación de los servicios.

NIVEL	NIVEL ACEPTACIÓN	REGISTRO	SEGUIMIENTO
EXTREMO	No Aceptable	Informes a la Alta Dirección	Mensual
ALTO		Informes a la Alta Dirección	Trimestral
MEDIO		Informes a la Alta Dirección	Trimestral
BAJO	Aceptable	Informes a la Alta Dirección	Semestral

La valoración de los riesgos se realiza multiplicando la calificación de la Probabilidad por la calificación del Impacto dando como resultado los niveles de severidad del riesgo:

Mapa de Calor



Nivel de severidad del riesgo:

BAJO	Aceptar riesgo
MEDIO	Aceptar o reducir riesgo
ALTO	Reducir, evitar, compartir riesgo
EXTREMO	Evitar, reducir, compartir riesgo

2. Clasificación del Riesgo

Existen dos (2) tipos de riesgo para su tratamiento, los cuales se detallan a continuación:

Riesgo Inherente (antes de controles): es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

El tratamiento se realiza mediante la definición de una serie de acciones o controles, los cuales tienen un responsable y una fecha para el seguimiento, buscando de esta forma asegurar la correcta administración de los riesgos. Esta información se puede evidenciar en el mapa de riesgos de la entidad.

Para esto, la Política de Riesgos en INFOTEP establece los principios para dar correcto tratamiento de los riesgos, mediante el establecimiento de planes de acción estratégicos y asegurando la continuidad del proceso.

Riesgo Residual (después de controles): El riesgo residual es el riesgo resultante después de aplicar los controles necesarios para su mitigación y prevenir su ocurrencia. El tratamiento de estos riesgos se clasifica de acuerdo con el nivel de severidad.

De acuerdo con la probabilidad e impacto de los riesgos y a los controles aplicados se evalúa el riesgo residual y dependiendo de este resultado se analiza si los riesgos (i) se asumen (ii) se reducen (iii) se comparten o transfieren, o (iv) se evitan.

Teniendo en cuenta lo anterior, INFOTEP ha establecido seguimientos con cierta periodicidad en cada uno de sus procesos de control, donde se evidencia también el responsable.

3. Tipos de control

Estratégicos: establece objetivos generales, controla el desempeño y los resultados de la entidad en su totalidad. Se basa en el ejercicio de planeación estratégica que está en cabeza de la oficina de Planeación.

Tácticos: miden y corrigen el desempeño para asegurar que los objetivos de la entidad y los planes establecidos para alcanzarlos se realicen. Entre los planes específicos que se llevan a cabo en la entidad encontramos: control presupuestal, cumplimiento de metas, establecimiento de estándares de calidad y cumplimiento en el avance de proyectos, los cuales están en cabeza del Comité Institucional de Gestión y Desempeño.

Operacionales: es el control sobre la ejecución de las tareas y las operaciones desempeñadas por el personal no administrativo de la entidad. Su acción es inmediata. Se evidencia en el control diario de ejecución de actividades.

4. Periodicidad para el seguimiento

Se deberá incluir la administración de riesgos dentro del sistema de gestión para facilitar la apropiación de este tema, y se seguirá realizando el seguimiento mediante reuniones específicas (RE) realizadas por los diferentes Grupos Internos de Trabajo de manera continua para todos los procesos cada trimestre. El cumplimiento de esta política, así como la aplicación de la metodología de administración de riesgos de la Entidad se realizará de la siguiente manera:

a) Anualmente se revisa el mapa de riesgos completo de la Entidad, en los plazos establecidos dentro del Plan Anticorrupción y de Atención al ciudadano de cada vigencia, para lo cual se tomará como insumo, las auditorías realizadas por Control Interno y Organismos de Control, así como lo reportado en las diferentes reuniones específicas (RE) e informes

presentados por los diferentes procesos a la Alta Dirección. Esta revisión será realizada con el acompañamiento de los líderes de procesos y de esta manera se ajustará el mapa de riesgos de acuerdo con los cambios normativos sectoriales y nacionales. El control de cambios del mapa de riesgos estará bajo la responsabilidad del encargado o responsable del Sistema de Gestión.
Responsable: Planeación con apoyo de los líderes de procesos.

b) El seguimiento se realizará cuatrimestralmente; dentro de los informes que se remitan a la Alta Dirección con los resultados del periodo y previo a esa fecha se deben realizar las reuniones específicas (RE), las cuales en su agenda incluirán el análisis de los riesgos, para hacer seguimiento a los mismos y revisar los controles por parte del equipo asistente a la reunión. Para alcanzar dicho objetivo, el equipo que haga parte de la RE debe conocer los riesgos y el estado actual de los mismos para participar activamente en cada reunión.
Responsable: Líderes de Procesos.

c) Presentar cuatrimestralmente los resultados del análisis de riesgos a la Alta Dirección, a través de los informes, con el fin de evidenciar si se materializó algún riesgo, si es necesario crear alguno nuevo o si se requiere eliminar alguno que con el tiempo no aplique a la entidad.
Responsable: Planeación con apoyo del encargado del Sistema de Gestión.

d) Fortalecer el cumplimiento de la presente política a través de capacitaciones establecidas dentro del Plan Anual de Capacitaciones de la entidad.
Responsable: Vicerrectoría Administrativa y Financiera

5. Niveles de responsabilidad sobre el seguimiento y evaluación

A partir de las líneas de defensa establecidas dentro del Modelo Integrado de Planeación y Gestión, las responsabilidades respecto la gestión, seguimiento y evaluación de los riesgos son las siguientes:

Línea de defensa	Responsables	Actividades
Línea Estratégica	Alta dirección y Comité Institucional de	• Establecer la Política de Administración del Riesgo • Específicamente el Comité Institucional de

	Coordinación de Control Interno.	Coordinación de Control Interno, evaluar y dar línea sobre la administración de los riesgos en la entidad • Realimentar a la Alta Dirección sobre el monitoreo y efectividad de la gestión del riesgo y de los controles. • Hacer seguimiento a su gestión, gestionar los riesgos y
Primera Línea	Líderes de procesos y sus grupos de trabajo	• Identificar y valorar los riesgos que pueden afectar el logro de los objetivos institucionales • Definir y diseñar los controles a los riesgos. • A partir de la política de administración del riesgo, establecer sistemas de gestión de riesgos y las responsabilidades para controlar riesgos específicos bajo la supervisión de la alta dirección. Con base a esto, establecer los mapas de riesgos.
		• Identificar y controlar los riesgos relacionados con posibles actos de corrupción en el ejercicio de sus funciones y el cumplimiento de sus objetivos, así como en la prestación del servicio y/o relacionados con el logro de los objetivos. Implementan procesos para identificar, disuadir y detectar fraudes; y revisan la exposición de la entidad al fraude con el auditor interno de la entidad.
Segunda Línea	Todos los funcionarios de la entidad	• Informar sobre la incidencia de los riesgos en el logro de objetivos y evaluar si la valoración del riesgo es la apropiada • Asegurar que las evaluaciones de riesgo y control incluyan riesgos de fraude • Monitorear cambios en el riesgo legal, regulatorio y de cumplimiento • Consolidar los seguimientos a los mapas de riesgo • Seguir los resultados de las acciones emprendidas para mitigar los riesgos, cuando haya lugar • Los supervisores de contratos deben realizar seguimiento a los riesgos de estos e informar las alertas respectivas
Tercera Línea	Jefe de Control Interno	• Asesorar en metodologías para la identificación y administración de los riesgos, en coordinación con la

		segunda línea de defensa • Identificar y evaluar cambios que podrían tener un impacto significativo en el SCI, durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna • Comunicar al Comité de Coordinación de Control Interno posibles cambios e impactos en la evaluación del riesgo, detectados en las auditorías • Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos claves de la entidad • Alertar sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas

6. Indicaciones especiales

El Jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento a la gestión del riesgo, verificando la efectividad de los controles de la siguiente manera:

– Primer seguimiento: Con corte al 30 de abril
– Segundo seguimiento: Con corte al 31 de agosto
– Tercer seguimiento: Con corte al 31 de diciembre

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web o en un lugar visible dentro de los diez (10) primeros días siguientes a la fecha de corte.

En especial deberá adelantar las siguientes actividades:

- Verificar la publicación del mapa de riesgos en la página web de la entidad.

- Seguimiento a la gestión del riesgo.

- Revisión de los riesgos y su evolución.

Acciones a seguir en caso de materialización de riesgos de corrupción.

- Informar a las autoridades de la ocurrencia del hecho de corrupción.
- Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
- Verificar si se tomaron las acciones y se actualizó el mapa de riesgos
- Llevar a cabo un monitoreo permanente

6. APLICABILIDAD

Aplica a todos los servidores de INFOTEP de tal manera que su accionar reduzca y/o disminuya la ocurrencia de los riesgos asociados a sus funciones.

La responsabilidad de los servidores públicos y demás colaboradores es llevar a cabo las directrices planteadas en esta política. Es un compromiso y responsabilidad de todos, conocer la Política y es su deber cumplirla y respetarla para el desarrollo de cualquier actividad o consulta

7. ACTUALIZACION

Este manual será actualizado cuando se presenten nuevas normativas y/o lineamientos establecidos por ley o la función pública o cuando la evaluación de los riesgos indique niveles extremos de los mismos de manera recurrente.

8. APROBACIÓN

Aprobado mediante Resolución 096 de 2020, en sesión del Comité de Gestión y Desempeño Institucional de 24 de agosto de 2020.