



SISTEMA INTEGRADO DE GESTIÓN Y DE CALIDAD

Código: ME-MC-M06

MEJORAMIENTO CONTINUO

Versión: 4

MANUAL DE GESTIÓN DEL RIESGO

Fecha: 09/11/2020

Pág. 1 de 30



MANUAL DE GESTION DEL RIESGO


	SISTEMA INTEGRADO DE GESTIÓN Y DE CALIDAD	Código: ME-MC-M06
	MEJORAMIENTO CONTINUO	Versión: 4
	MANUAL DE GESTIÓN DEL RIESGO	Fecha: 09/11/2020
		Pág. 2 de 30

TABLA DE CONTENIDO

INTRODUCCIÓN.....	4
1. OBJETIVO	5
2. ALCANCE	5
3. DEFINICIONES.....	5
4. GENERALIDADES	7
4.1. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS	8
4.2. POLÍTICAS GENERALES DE ADMINISTRACIÓN DEL RIESGO	9
4.3. GESTIÓN DEL RIESGO.....	9
5. PROCESO DE ADMINISTRACIÓN DE RIESGOS.....	10
5.1. IDENTIFICACIÓN DE LOS RIESGOS.	10
5.2. ESTABLECIMIENTO DEL CONTEXTO PARA LA GESTIÓN DEL RIESGO.	11
5.2.1. Identificación de activos de seguridad de la información.....	11
5.3. Identificación de Riesgos de Corrupción.....	13
5.4. TIPOLOGÍA DE RIESGOS:.....	14
5.5. ANÁLISIS DEL RIESGO.....	15
5.6. DISEÑO DE CONTROLES.	21
5.7. EVALUACIÓN DE CONTROLES.....	21
5.7.1. Evaluación del Diseño del Control.	21
5.7.2. Evaluación de la ejecución del control.....	23
5.7.3 Establecimiento de acciones para fortalecer el control evaluado.	23
5.7.4. Solidez del conjunto de controles.....	24
5.7.5. Desplazamiento del riesgo inherente para calcular el riesgo residual.	25



SISTEMA INTEGRADO DE GESTIÓN Y DE CALIDAD

Código: ME-MC-M06

MEJORAMIENTO CONTINUO

Versión: 4


MANUAL DE GESTIÓN DEL RIESGO

Fecha: 09/11/2020

Pág. 3 de 30

|


5.8. MANEJO DEL RIESGO.....	26
5.9. MONITOREO.....	27
6. BIBLIOGRAFÍA.....	29
7. CONTROL DE CAMBIOS	30
8. CONTROL DE APROBACION	30

	SISTEMA INTEGRADO DE GESTIÓN Y DE CALIDAD	Código: ME-MC-M06
	MEJORAMIENTO CONTINUO	Versión: 4
	MANUAL DE GESTIÓN DEL RIESGO	Fecha: 09/11/2020 Pág. 4 de 30

INTRODUCCIÓN

Este manual contiene la metodología para llevar a cabo la identificación, análisis y valoración del riesgo dentro de cada uno de los procesos, iniciando con la identificación del contexto estratégico, además de establecer los actores y responsables del proceso de administración del riesgo y define las políticas generales de administración del riesgo aplicables para TEVEANDINA – Canal Trece.

Para la elaboración del presente Manual se tomó como referencia los lineamientos del Departamento Administrativo de la Función Pública DAFP, establecidos mediante la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas v4 del DAFP, la Norma NTC ISO 31000:2011. Gestión del Riesgo

	SISTEMA INTEGRADO DE GESTIÓN Y DE CALIDAD	Código: ME-MC-M06
	MEJORAMIENTO CONTINUO	Versión: 4
	MANUAL DE GESTIÓN DEL RIESGO	Fecha: 09/11/2020
		Pág. 5 de 30

1. OBJETIVO

Establecer los lineamientos generales para una adecuada gestión del riesgo en el Canal, a partir de la implementación de cada una de sus etapas, de tal manera que se cuente con información confiable para la toma de decisiones y gestión de los procesos.

2. ALCANCE

Aplica para los riesgos considerados en el mapa de riesgos institucional, en el mapa de riesgos por proceso y para los riesgos de corrupción.

3. DEFINICIONES

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.

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 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: 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 persona.

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.

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

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

	SISTEMA INTEGRADO DE GESTIÓN Y DE CALIDAD	Código: ME-MC-M06
	MEJORAMIENTO CONTINUO	Versión: 4
	MANUAL DE GESTIÓN DEL RIESGO	Fecha: 09/11/2020
		Pág. 6 de 30

Probabilidad: Se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de Frecuencia o Factibilidad.

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

Riesgo Inherente: Es aquel 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.

Política para la gestión del riesgo: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.

Mapa de riesgos: Documento con la información resultante de la gestión del riesgo.

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.

Control: Medida que modifica el riesgo (Procesos, políticas, dispositivos, prácticas u otras acciones)


Integridad: Propiedad de exactitud y completitud.

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

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

Apetito de riesgo: Magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener,

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.

	SISTEMA INTEGRADO DE GESTIÓN Y DE CALIDAD	Código: ME-MC-M06
	MEJORAMIENTO CONTINUO	Versión: 4
	MANUAL DE GESTIÓN DEL RIESGO	Fecha: 09/11/2020 Pág. 7 de 30

Confidencialidad: Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidad o procesos no autorizados.

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

4. GENERALIDADES


El manual toma como base fundamental los lineamientos establecidos por el Departamento Administrativo de la Función Pública (DAFP), en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas y lo indicado en el Modelo Estándar de Control Interno.

Para ello, Teveandina Ltda – Canal Trece, adopta esta metodología de administración del riesgo con el interés de formalizar y fortalecer el compromiso de la entidad en el tema, al estar conscientes que una adecuada gestión de riesgos permite:

- Aumentar la probabilidad de alcanzar los objetivos
- Establecer una base confiable para la toma de decisiones y la planificación.
- Preparar a la organización para eventos no esperados “Evitar sorpresas”
- Cuidar nuestros principales activos: Los recursos de la Nación, las Personas
- Prevenir amenazas y aprovechar oportunidades
- Mejorar la presentación de informes obligatorios y voluntarios
- Mejorar el aprendizaje organizacional

Los principios de la gestión de riesgos son:

- Crear y proteger el valor contribuyendo al logro demostrable de los objetivos y a la mejora del desempeño
- Ser parte integral de todos los procesos de la organización, no una actividad independiente

	SISTEMA INTEGRADO DE GESTIÓN Y DE CALIDAD	Código: ME-MC-M06
	MEJORAMIENTO CONTINUO	Versión: 4
	MANUAL DE GESTIÓN DEL RIESGO	Fecha: 09/11/2020
		Pág. 8 de 30


- Ser parte de la toma de decisiones
- Abordar explícitamente la incertidumbre
- Debe ser sistemática, estructurada y oportuna contribuyendo a la eficiencia y resultados consistentes, comparables y confiables
- Establecer la mejor información disponible basándose en datos históricos, experiencia, retroalimentación, observación, previsiones y examen de expertos
- Intervención por aquellos que toman decisiones en todos los niveles de la organización, garantizando de esta forma que sea transparente e inclusiva
- Alinear el contexto externo e interno y el perfil de riesgo de la organización a la gestión del riesgo.
- Ser parte de las responsabilidades de la alta dirección
- Considerar los factores humanos y culturales
- Es dinámica, reiterativa y receptiva al cambio
- Facilitar la mejora continua en la organización

4.1. POLITICA DE ADMINISTRACIÓN DE RIESGOS

TEVEANDINA LTDA – Canal Trece, está comprometida con la administración efectiva de riesgos que incluya los riesgos de corrupción, riesgos de seguridad informática, riesgos por proceso, identificándolos y promoviendo las acciones y controles necesarios que le permitan al canal mitigarlos, evitando que se materialicen y afecten negativamente los logros y los objetivos institucionales.

La publicación del mapa integrado de riesgos se realiza de acuerdo con las disposiciones legales.

Anualmente, en el último trimestre del año se revisarán los riesgos de gestión y de corrupción por proceso identificados de acuerdo con los parámetros vigentes definidos por el DAFP

	SISTEMA INTEGRADO DE GESTIÓN Y DE CALIDAD	Código: ME-MC-M06
	MEJORAMIENTO CONTINUO	Versión: 4
	MANUAL DE GESTIÓN DEL RIESGO	Fecha: 09/11/2020
		Pág. 9 de 30

4.2. POLÍTICAS GENERALES DE ADMINISTRACIÓN DEL RIESGO

La Alta Dirección, la Dirección de Control Interno y Evaluación y control de Gestión se compromete a:

- Liderar y apoyar la Administración de Riesgos en todos los procesos, riesgos de corrupción, programas, proyectos, y/o dependencias de la institución; todas las acciones conducentes a ello estarán acordes con la legislación vigente y la normatividad interna. Pondrá especial atención en el manejo de los riesgos de corrupción que puedan afectar a la organización.
- Establecer, dar a conocer y mantener las estrategias de mitigación o tratamiento de los riesgos, como pilares fundamentales en la administración de los riesgos.
- Divulgar en toda la Institución la misión, visión, estrategias, políticas, responsabilidades y procedimientos de manera que todos los funcionarios se sientan involucrados y compartan su responsabilidad en el proceso de administración de riesgos.
- Vigilar el cumplimiento y entendimiento de las normas, políticas y procedimientos tendientes a minimizar el riesgo en cada una de las áreas expuestas en la Institución.

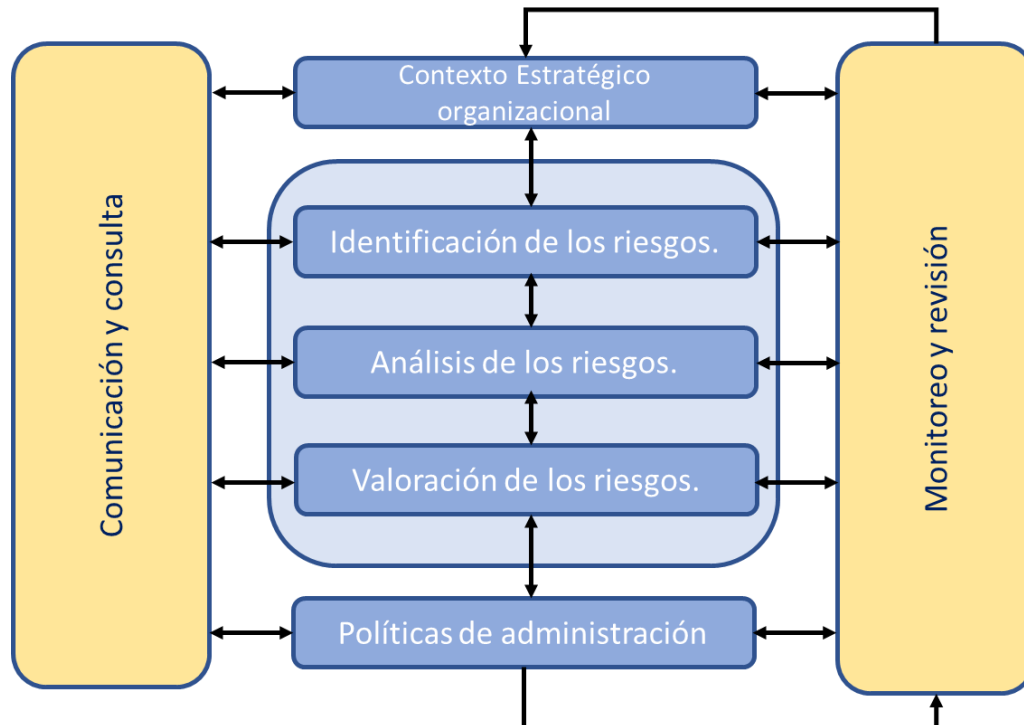
4.3. GESTIÓN DEL RIESGO

El mapa integrado de riesgos que contiene los riesgos de gestión y de corrupción, se debe:

- Elaborar anualmente por cada responsable de los procesos, junto con su equipo.
- Elaborar y consolidar con el liderazgo de planeación junto a los líderes de cada proceso.
- Realizar el seguimiento Control Interno con corte a las siguientes fechas: 30 de abril, 31 de agosto y 31 de diciembre.
- Publicar en la página web, a más tardar el día 31 del mes de enero y realizar su divulgación interna y externa a través de la sección de Transparencia y Acceso a la Información Pública.

5. PROCESO DE ADMINISTRACIÓN DE RIESGOS.


A continuación, se presenta cada una de las etapas a desarrollar durante la administración del riesgo.



5.1. IDENTIFICACIÓN DE LOS RIESGOS.

Teveandina Ltda. – Canal Trece identifica las fuentes de riesgo, las áreas de impacto, los eventos, causas y consecuencias potenciales generando una lista exhaustiva con base en los eventos que puedan crear, aumentar, prevenir, degradar, acelerar o retrasar el logro de sus objetivos.

Para ello incluye riesgos sin importar si su origen está o no bajo el control de la entidad, aun cuando su causa pueda no ser evidente. Para ello se realiza una lluvia de ideas donde se analizan los efectos que riesgo podría causar, así como su impacto y probabilidad basándose en situaciones que hayan ocurrido en los últimos 5 años. Para determinar las consecuencias se toma un rango amplio que abarca desde el peor de los casos (materialización del riesgo) hasta la consecuencia más baja.

	SISTEMA INTEGRADO DE GESTIÓN Y DE CALIDAD	Código: ME-MC-M06
	MEJORAMIENTO CONTINUO	Versión: 4
	MANUAL DE GESTIÓN DEL RIESGO	Fecha: 09/11/2020
		Pág. 11 de 30

Para identificar los riesgos, se realizan mesas de trabajo por proceso donde se lista una serie de posibles eventos que se adecuen de acuerdo con los objetivos de su proceso y su entorno. Esta información es analizada por cada proceso, realizando una depuración de los riesgos que no los afectan y determinando su impacto y probabilidad basados en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del DAFP.

5.2. ESTABLECIMIENTO DEL CONTEXTO PARA LA GESTIÓN DEL RIESGO.

Para establecer el contexto del proceso para la gestión del riesgo, la alta dirección deberá articular sus objetivos, estrategias, alcance, metodologías y los parámetros de las actividades de la organización estableciendo los contextos externos (políticos, económicos y financieros, sociales y culturales, tecnológicos, ambientales, legales y reglamentarios), los contextos internos (financieros, personal, procesos, tecnología, estratégicos, comunicación interna) y los contextos del proceso (diseño del proceso, interacciones con otros procesos, transversalidad, procedimientos asociados, responsables del proceso, comunicación entre los procesos y activos de seguridad digital del proceso)

5.2.1. Identificación de activos de seguridad de la información. Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos que utiliza la organización para funcionar en el entorno digital tales como: aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información -TI, tecnologías de operación -TO.

Para identificar los activos la primera línea de defensa deberá realizar los siguientes pasos:

- Listar los activos por cada proceso
- Identificar el dueño de los activos
- Clasificar los activos
- Clasificar la información
- Determinar la criticidad del activo
- Identificar si existe infraestructura critica cibernética

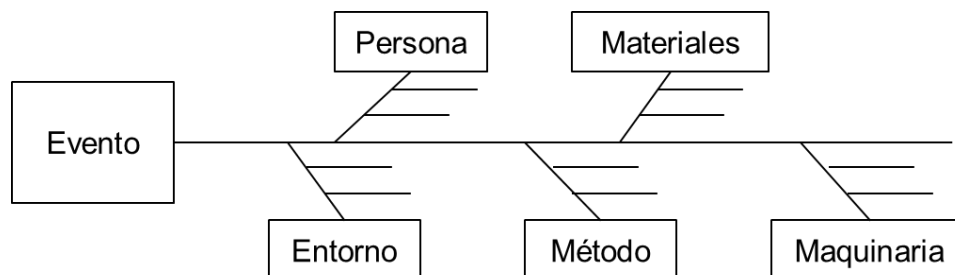
TÉCNICAS PARA LA IDENTIFICACIÓN DE LOS RIESGOS

Las causas, son el aspecto que se debe eliminar o mitigar para que el riesgo no se materialice, mediante la definición de controles efectivos. Para realizar el análisis de las causas en la etapa de identificación o incluso cuando un riesgo se ha materializado, existen varias técnicas que serán analizadas a continuación:

5.3.1. Lluvia de Ideas. De una manera organizada y en un período mu y breve de tiempo los actores que intervienen en el proceso lanzan creativamente diferentes ideas teniendo en cuenta el contexto.

- Debe haber un moderador que tome nota y que organice las exposiciones de todos los participantes, indicando el tiempo que cada cual tiene para presentar sus ideas.
- Es más importante la cantidad de ideas que la calidad de las mismas. Todas las ideas son valiosas para el proceso de recopilación de información.
- No se deben calificar las ideas como buenas o malas, son simplemente puntos de vista que capitalizados pueden brindar alternativas no consideradas.
- Es importante soportarse en las ideas de los otros. Es decir, agregar valor a las apreciaciones de otros o considerar situaciones a partir de las mismas.
- El análisis de las ideas se debe realizar al final, por el moderador, quien las organizará y las expondrá a manera de resultado.
- Todos deben participar de manera equitativa, es importante no fijar la atención en pocos participantes, ni mantenerse en la palabra sin dar la oportunidad a otro de expresar sus ideas.

5.3.2. Espina de pescado. Es un método que permite visualizar de manera estructurada todas las causas posibles del riesgo.



- La causa principal debe ir pegada a la “cabeza”.
- Pregúntese, ¿Qué podría causar el problema?
- Coloque las causas en cada una de las áreas

5.3.3. Método de la escalera (5 porqués). Es un método basado en realizar preguntas para explorar las relaciones de causa-efecto que generan un problema en particular. El objetivo final de los 5 Porqué 's es determinar la causa raíz de un defecto o problema.

5.3.4. Recomendación del DAFP. Las preguntas clave para identificar los riesgos en la entidad son:


- ¿Qué puede suceder? Identificar la afectación del cumplimiento del objetivo estratégico o del proceso según sea el caso.
- ¿Cómo puede suceder? Establecer las causas a partir de los factores determinados en el contexto.
- ¿Cuándo puede suceder? Determinar de acuerdo con el desarrollo del proceso.
- ¿Qué consecuencias tendría su materialización? Determinar los posibles efectos por la materialización de un riesgo.

5.3. Identificación de Riesgos de Corrupción.

Los riesgos de corrupción deben ser establecidos sobre los procesos de la entidad. Para facilitar su identificación y no confundirlo con otra clase de riesgo la entidad se siguen las recomendaciones de la Secretaría de Transparencia de la Presidencia de la Republica, teniendo en cuenta la siguiente matriz:

MATRIZ DEL RIESGO DE CORRUPCIÓN				
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

Si se marca con una X las opciones de cada casilla para la Descripción del Riesgo significa que el riesgo identificado es de corrupción.

	SISTEMA INTEGRADO DE GESTIÓN Y DE CALIDAD	Código: ME-MC-M06
	MEJORAMIENTO CONTINUO	Versión: 4
	MANUAL DE GESTIÓN DEL RIESGO	Fecha: 09/11/2020
		Pág. 14 de 30

5.4. TIPOLOGÍA DE RIESGOS:

La tipología de riesgos depende de la misión de la entidad y de las normas que regulan su operación, de los sistemas de gestión que implemente, entre otros aspectos y se clasifican de la siguiente manera:

- **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 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.
- **Riesgos tecnológicos:** posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnología (hardware, software, redes, etc.) de una entidad.
- **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 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 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 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.

5.4.4. Errores frecuentes en la identificación de los riesgos.

- **Referencia circular:** Esto es, identificar un riesgo simplemente como el contrario de un objetivo. Ejemplo: si el objetivo es “asegurarse que todas las facturas son aprobadas antes de su pago”, el riesgo se identifica como “las facturas pueden ser pagadas antes de ser aprobadas”. Esto agrega muy poco valor al proceso de identificación de riesgo.

- **Iniciar la redacción con palabras negativas:** Para la redacción de un riesgo se debe evitar iniciar con palabras negativas como “No, Que no, etc”.

5.5. ANÁLISIS DEL RIESGO.

El análisis del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo. La primera puede ser medida con criterios de Frecuencia, si se ha materializado o no.

Tabla de Probabilidad.

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

En caso de que para un riesgo identificado no se cuente con datos históricos sobre las materializaciones que haya presentado en un periodo de tiempo. Se deberá calificar la probabilidad en términos de factibilidad utilizando la siguiente matriz diseñada por el DAFP:

No.	Riesgo	P1	P2	P3	P4	P5	P6	TOT	PROM
1	Riesgo Identificado # 1								
2	Riesgo Identificado # 2								
3	Riesgo Identificado # 3								

Convenciones:

No. Número consecutivo del riesgo - P1. Participante 1 – TOT: Total puntaje – PROM: Promedio

Tabla de impacto.

Nivel	Descriptor	Impacto Cuantitativo	Impacto Cualitativo
1	Insignificante	<p>Impacto que afecte la ejecución presupuestal en un valor menor o igual al 0,5%</p> <p>Perdida de cobertura en la prestación de servicios de la entidad menor o igual al 0,5%</p> <p>Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor menor o igual al 0,5%</p> <p>Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor menor o igual al 0.5% del presupuesto general de la entidad</p>	<p>No hay Interrupción de las operaciones de la Entidad</p> <p>No se generan sanciones económicas o administrativas</p> <p>No se afecta la Imagen institucional de forma significativa</p>
2	Menor	<p>Impacto que afecte la ejecución presupuestal en un valor menor o igual al 1%</p> <p>Perdida de cobertura en la prestación de servicios de la entidad menor o igual al 1%</p> <p>Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor menor o igual al 1%</p> <p>Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor menor o igual al 1% del presupuesto general de la entidad</p>	<p>Interrupción de las operaciones de la Entidad por algunas horas</p> <p>Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias</p> <p>Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos</p>
3	Moderado	<p>Impacto que afecte la ejecución presupuestal en un valor mayor o</p>	<p>Interrupción de las operaciones de la Entidad por más de un (1) día</p>

		<p>igual al 5%</p> <p>Perdida de cobertura en la prestación de servicios de la entidad mayor o igual al 5%</p> <p>Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor mayor o igual al 5%</p> <p>Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor mayor o igual al 5% del presupuesto general de la entidad</p>	<p>Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad</p> <p>Inoportunidad en la información ocasionando retrasos en la atención a los usuarios</p> <p>Reproceso de actividades y aumento de carga operativa</p> <p>Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos</p> <p>Investigaciones penales, fiscales o disciplinarias</p>
4	Mayor	<p>Impacto que afecte la ejecución presupuestal en un valor mayor o igual al 20%</p> <p>Perdida de cobertura en la prestación de servicios de la entidad mayor o igual al 20%</p> <p>Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor mayor o igual al 20%</p> <p>Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor mayor o igual al 20% del presupuesto general de la entidad</p>	<p>Interrupción de las operaciones de la Entidad por más de dos (2) días</p> <p>Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta</p> <p>Sanción por parte del ente de control y otro ente regulador</p> <p>Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno</p> <p>Imagen institucional afectada en el orden nacional o regional por incumplimiento en la prestación del servicio a los usuarios o ciudadanos</p>
5	Catastrófico	<p>Impacto que afecte la ejecución presupuestal en un valor mayor o igual al 50%</p> <p>Perdida de cobertura en la prestación</p>	<p>Interrupción de las operaciones de la Entidad por más de cinco (5) días o cierre indefinido o total de la entidad.</p>

	de servicios de la entidad mayor o igual al 50%	Pérdida de información crítica para la entidad que no se puede recuperar
	Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor mayor o igual al 50%	Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal
	Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor mayor o igual al 50% del presupuesto general de la entidad	Sanciones por parte de un ente de control u otro ente regulador

Tabla de Impacto para Riesgos de Corrupción

No.	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SI	NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		

15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		
Responder afirmativamente de UNA a CINCO preguntas(s) genera un impacto moderado Responder afirmativamente de SEIS a ONCE preguntas genera un impacto Mayor Responder Afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico			
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad		
CASTRÓFICO	Genera consecuencias desastrosas para la entidad		

Para el impacto de los riesgos de corrupción se tendrán en cuenta solamente en los niveles moderado, mayor y catastrófico, dado que estos riesgos siempre serán significativos.

Mapa de Calor o Matriz de calificación, evaluación y respuesta a los riesgos.


Se obtiene ubicando el grado de calificación de la probabilidad y el impacto definidos para el riesgo y determina la zona de riesgo donde se ubicará el riesgo inherente.

Probabilidad	Impacto				
	Insignificante(1)	Menor(2)	Moderado(3)	Mayor(4)	Catastrófico(5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi seguro (5)	A	A	E	E	E

Tabla de Valoración del riesgo.

Tipo de efecto impacto	Estratégico	Operativo	Financiero	Cumplimiento	Tecnología	Imagen Reputación	Corrupción
Insignificante	Afecta el cumplimiento de algunas actividades del Plan Estratégico	Afecta a una actividad concreta del proceso / área	El impacto en el presupuesto del Canal es insignificante	Genera una alerta de incumplimiento	Genera interrupción en una actividad del proceso	Afecta la credibilidad - confianza de un proceso - área del Canal	
Menor	Afecta el cumplimiento de alguna iniciativa estratégica	Afecta varias actividades del proceso / área	Afecta hasta el 20% presupuesto del Canal	Genera un requerimiento formal por parte del usuario / cliente / parte interesada	Genera interrupción en varias actividades del proceso / área	Afecta al interior del Canal la credibilidad - confianza de un proceso	
Moderado	Afecta el cumplimiento de las metas de un grupo de procesos	Afecta la interrelación de procesos - áreas	Afecta hasta el 30% presupuesto del Canal	Genera interrupciones en el desarrollo de las actividades	Genera interrupción significativa en el desarrollo de las actividades de un proceso - áreas	Afecta la credibilidad - confianza de usuarios clientes externos, respecto a un proceso - área del Canal	Afectación parcial al proceso y a la dependencia Genera a medianas consecuencias para la entidad.
Mayor	Afecta el cumplimiento de objetivos estratégicos	Afecta ejecución de procesos misionales - estratégicos	Afecta hasta el 50% presupuesto del Canal	Genera investigaciones disciplinarias, y/o fiscales y/o penales	Genera interrupción entre la interacción de procesos - áreas	Afecta la credibilidad - confianza de los procesos misionales - área del Canal	Impacto negativo de la Entidad Genera altas consecuencias para la entidad.
Catastrófico	Afecta el cumplimiento de metas que pueden afectar el Sector	Genera interrupción significativa de procesos misionales	Afecta más del 50% presupuesto del Canal	Genera sanciones	Genera interrupción significativa de la prestación del servicio	Afecta la imagen del Canal - Sector	Consecuencias desastrosas sobre el sector Genera consecuencias desastrosas para la entidad.

Nota: A estos riesgos inicialmente identificados se les conocerá como Riesgos Inherentes y pueden afectar el cumplimiento de los objetivos estratégicos y de cada proceso, es importante entonces definir las causas que pueden dar origen a la materialización de un riesgo, teniendo en cuenta que para cada causa identificada se debe diseñar también un control. Para efectos de la matriz de riesgos consolidada las

	SISTEMA INTEGRADO DE GESTIÓN Y DE CALIDAD	Código: ME-MC-M06
	MEJORAMIENTO CONTINUO	Versión: 4
	MANUAL DE GESTIÓN DEL RIESGO	Fecha: 09/11/2020 Pág. 21 de 30

causas deberán manejarse en celdas separadas. Importante tener en cuenta que un control puede ser tan eficiente que podría mitigar varias causas.

5.6. DISEÑO DE CONTROLES.

Para definir correctamente un control que pueda mitigar las causas que dan origen a un riesgo es importante tener en cuenta las siguientes variables desde la redacción del control:

- Responsable de llevar a cabo la actividad de control
- Periodicidad para su ejecución
- Propósito del Control
- Establecer como se realiza la actividad de control
- Hay que indicar que pasa con las observaciones resultantes de ejecutar el control
- Evidenciar la ejecución del control (registro)

Nota: Evitar asignar procesos o áreas como responsables de las actividades de control y asignarlos a un cargo específico. El control debe tener un propósito (verificar, validar, revisar etc.). Se deben realizar seguimientos periódicos y estos deben ser documentados dejando evidencia de control en la periodicidad establecida. Para el caso específico de Teveandina Ltda. Canal Trece y debido a la naturaleza de sus procesos misionales la periodicidad de los riesgos podrá ser abierta o específica.

5.7. EVALUACIÓN DE CONTROLES.

Permite determinar en qué medida los controles identificados aportan para disminuir los niveles de probabilidad e impacto del riesgo.

5.7.1. Evaluación del Diseño del Control.

Para evaluar el diseño de un control se deberá tener en cuenta la siguiente tabla y sumar sus calificaciones para determinar si el diseño es fuerte, moderado o débil.

Tabla de variables y puntajes para el análisis y evaluación del diseño del control para la mitigación de los riesgos.

Apellido	Nombre	Criterio de Evaluación	Aspecto a Evaluar en el Diseño del Control	Opciones de Respuesta		Puntaje
		1. Responsable	¿Existe un responsable asignado a la ejecución del control?	Asignado	No Asignado	Asignado: 15 No Asignado: 0
			¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado	Inadecuado	Adecuado: 15 Inadecuado: 0
		2. Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna	Inoportuna	Oportuna: 15 Inoportuna: 0
		3. Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, Ej.: verificar, validar, cotejar, comparar, revisar, etc.?	Prevenir o Detectar	No es un control	Prevenir: 15 Detectar: 10 No es un control: 0
		4. Como se realiza la actividad de control	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	Confiable	No confiable	Confiable: 15 No confiable: 0
		5. Qué pasa con las observaciones o desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven oportunamente	No se investigan y resuelven oportunamente.	Se investigan y resuelven Oportunamente: 15 No se investigan y resuelven oportunamente: 0
		6. Evidencia de la ejecución del control	¿Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión?	Completa	Incompleta / no existe	Completa: 10 Incompleta: 5 No existe: 0

Después de calificar la tabla anterior, se deben sumar los puntajes según las opciones de respuesta seleccionada para determinar el rango de calificación del diseño de la siguiente manera:

Tabla de variables y puntajes para el análisis y evaluación del diseño del control para la mitigación de los riesgos.

Rango de Calificación del Diseño	Resultado – Peso en la Evaluación del Diseño del Control
Fuerte	96 a 100
Moderado	86 a 95
Débil	0 a 85

5.7.2. Evaluación de la ejecución del control.

Aunque la calificación en el diseño del control sea fuerte, se debe evaluar también la ejecución del control ya que no basta con solo tener el control bien diseñado. La organización debe asegurar la ejecución de los controles por medio de líderes de proceso y los gerentes públicos determinando la periodicidad de medición de estos para que de esta forma la auditoría interna o control interno pueda confirmar que se realizaron dichas actividades y según este documento se pueda determinar el rango de calificación de la ejecución del control según los criterios de la siguiente tabla:

Tabla de variables y puntajes para el análisis y evaluación del diseño del control para la mitigación de los riesgos.

Rango de Calificación de la Ejecución	Resultado – Peso en 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.

5.7.3 Establecimiento de acciones para fortalecer el control evaluado.

Teniendo la calificación de la evaluación del diseño y ejecución del control se deberá evaluar la solidez individual de cada control para establecer posteriormente si se deben o no realizar acciones de mejora para fortalecer el control evaluado. Dicha evaluación se realiza ingresando los rangos de calificación obtenidos por control en la siguiente tabla:

Tabla de evaluación a la solidez individual de cada control

Peso del Diseño de cada Control	Peso de la Ejecución de cada Control	Solidez Individual de cada Control Fuerte: 100 Moderado: 50 Débil: 0	Debe establecer acciones de mejora para Fortalecer el Control SI / NO
Fuerte: Calificación entre 96 y 100	Fuerte	Fuerte + Fuerte = Fuerte	NO
	Moderado	Fuerte + Moderado = Moderado	SI
	Débil	Fuerte + Débil = Débil	SI
Moderado: Calificación entre 86 y 95	Fuerte	Moderado + Fuerte = Moderado	SI
	Moderado	Moderado + Moderado = Moderado	SI
	Débil	Moderado + Débil = Débil	SI
Débil: Calificación entre 0 y 85	Fuerte	Débil + Fuerte = Débil	SI
	Moderado	Débil + Moderado = Débil	SI
	Débil	Débil + Débil = Débil	SI

5.7.4. Solidez del conjunto de controles.

Para evaluar la solidez del conjunto de controles se deberá calcular el promedio de la solidez individual de cada control determinando si es fuerte, moderado o débil según la información de la siguiente tabla.

Tabla de evaluación a la solidez en conjunto de controles.

Rango de Calificación de la solidez en conjunto de controles	Resultado – Peso en la solidez en 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.

5.7.5. Desplazamiento del riesgo inherente para calcular el riesgo residual.

La mayoría de los controles que se diseñan son para disminuir la probabilidad de que un riesgo se materialice y muy pocos están dirigidos al impacto. Pero si no existieran dichos controles sobre la probabilidad, el impacto por riesgos que llegasen a materializarse sería mayor. Es por tal razón que para la elaboración de la matriz de desplazamiento del riesgo se deberá evaluar si el control ayuda a disminuir el impacto o la probabilidad y se calificará teniendo en cuenta que de manera indirecta también disminuirá el impacto.

Tabla de desplazamiento del riesgo inherente para el cálculo del riesgo residual.

Solidez de conjunto de los controles.	Controles que ayudan a disminuir la probabilidad	Controles que 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

Para los riesgos de corrupción solamente podrá haber disminución de la probabilidad ya que el impacto siempre será significativo.

En caso de encontrarse una solidez de conjunto de control Débil no disminuirá la probabilidad o el impacto asociado al riesgo.

En la siguiente matriz se ilustra el mapa de riesgo inherente antes de controles, y como se deberán disminuir las probabilidades e impactos después de los controles.

Probabilidad	Impacto				
	Insignificante(1)	Menor(2)	Moderado(3)	Mayor(4)	Catastrófico(5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi seguro (5)	A	A	E	E	E



Tabla de criterios sobre la zona de riesgo.

Zona de Riesgo	Color	Descripción
Baja		Aceptar el riesgo
Moderada		Aceptar el riesgo, Reducir el riesgo.
Alta		Reducir el riesgo, Evitar el riesgo, Compartir o transferir.
Extrema		Evitar el riesgo, Reducir el riesgo, Compartir o transferir.

5.8. MANEJO DEL RIESGO.

El objetivo es definir las acciones a realizar para atender los riesgos, según la priorización dada por el grado de exposición, estas deben ser factibles y efectivas.

Una vez determinada la zona donde está ubicado el riesgo, y dependiendo de las opciones de manejo, se deben formular las acciones orientadas al mejoramiento y fortalecimiento de los controles identificados; estas acciones se incluyen dentro de un plan de manejo.


5.7.1. Opciones de manejo.

- **Aceptar el riesgo:** aceptar la pérdida residual probable. (en ningún caso se podrá aceptar un riesgo de corrupción)
- **Reducir el riesgo:** implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección).
- **Evitar el riesgo:** tomar las medidas encaminadas a prevenir su materialización.
- **Compartir o transferir el riesgo:** reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o mediante otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido.


5.9. MONITOREO.

El monitoreo y revisión de la gestión de riesgos, está alineado con la dimensión de Control interno del MIPG de “Control Interno” que se desarrolla con el MECI a través de un esquema de asignación de responsabilidades y roles, distribuido de la siguiente manera:

LÍNEA DE MONITOREO Y REVISIÓN	RESPONSABILIDAD	ROL
Línea Estratégica	Alta Dirección y Comité Institucional de Coordinación de Control Interno	Tendrá la responsabilidad de definir el marco general para la gestión del riesgo (política de administración del riesgo) y garantizar el cumplimiento de los planes de la entidad. Analiza los riesgos y amenazas institucionales al cumplimiento de los planes estratégicos (objetivos, metas, indicadores)
Primera Línea de Defensa	Líderes de proceso y sus equipos de trabajo.	Garantizan la gestión del día a día, en conjunto con sus equipos de trabajo. Se encarga de identificar, evaluar, controlar y mitigar los riesgos. Son responsables de implementar acciones correctivas y detectar fallas en los controles.
Segunda Línea de Defensa	Gerencia, jefe de planeación, supervisores e interventores de contratos y/o proyectos.	Corresponde establecer mecanismos que les permitan ejecutar un seguimiento o autoevaluación permanente de la

	SISTEMA INTEGRADO DE GESTIÓN Y DE CALIDAD	Código: ME-MC-M06
	MEJORAMIENTO CONTINUO	Versión: 4
	MANUAL DE GESTIÓN DEL RIESGO	Fecha: 09/11/2020 Pág. 28 de 30

		gestión, orientando y generando alertas a la primera línea de defensa. Supervisa la implementación de prácticas de gestión eficaces por parte de la primera línea.
Tercera Línea de Defensa	Control Interno y auditoría interna.	A través de un enfoque basado en riesgos, proporciona aseguramiento sobre la eficacia de la gestión del riesgo y control interno a la alta dirección.

	SISTEMA INTEGRADO DE GESTIÓN Y DE CALIDAD	Código: ME-MC-M06
	MEJORAMIENTO CONTINUO	Versión: 4
	MANUAL DE GESTIÓN DEL RIESGO	Fecha: 09/11/2020 Pág. 29 de 30

6. BIBLIOGRAFÍA

DAFP. (2018). GUIA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DEL RIESGO Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS. Bogotá D.C.: Departamento Administrativo de la Función Pública. (DAFP)

ICONTEC Internacional. (2011). NORMA TÉCNICA COLOMBIANA GTC 137. GESTIÓN DEL RIESGO. VOCABULARIO. Bogotá D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

ICONTEC Internacional. (2011). NORMA TÉCNICA COLOMBIANA NTC ISO 31000. GESTIÓN DEL RIESGO. PRINCIPIOS Y DIRECTRICES. Bogotá D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

ICONTEC Internacional. (2013). NORMA TÉCNICA COLOMBIANA NTC-IEC/ISO 31010. GESTION DE RIESGOS. TÉCNICAS DE VALORACIÓN DEL RIESGO. Bogotá D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

7. CONTROL DE CAMBIOS

Versión	FECHA	DESCRIPCIÓN DEL CAMBIO	RESPONSABLE
0	Marzo 2015	Documento Original	Asesor Planeación y Calidad
1	31-05-2016	Se incluye descripción de herramientas para el análisis de causas, se incluye numeral de roles y responsabilidades, se amplía el alcance a los riesgos de corrupción.	Asesor Planeación y Calidad
2	13/09/2018	Actualización de la política de gestión de riesgos, actualización del manual bajo los parámetros actualizados de la Norma Iso 31000 y DAFP	Líder de Planeación
3	15/05/2019	Actualización del manual bajo los parámetros de la guía del DAFP y la Norma ISO 31000, contenido agregado y bibliografía.	Líder de Planeación
4	09/11/2020	Actualización del manual bajo los parámetros de la guía del DAFP	Líder de Planeación

8. CONTROL DE APROBACION

Elaboró:	Aprobó:
Giovanni Andrés Méndez – Juan Sebastian Monje	Gina Alejandra Albarracín Barrera
Líder de Planeación – Profesional de Planeación	Gerente
Fecha de aprobación: 09/11/2020	