POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

Elaborado por:	Revisado por:	Aprobado por:
Asesor(a) Planeación	Asesor(a) Control Interno	Rector(a)

1. OBJETIVO

Implementar la metodología de Administración de los Riesgos de Gestión, de Corrupción y Seguridad Digital que permita gestionar de manera efectiva los riesgos que afectan el logro de los objetivos estratégicos y de proceso, determinando roles y responsabilidades por cada línea de defensa mediante la identificación, análisis y evaluación de los riesgos y establecer los mecanismos de comunicación de la política de riesgos en todos los niveles de la IUCMC.

2. ALCANCE

Aplica a todos los procesos establecidos en el Mapa de Proceso Institucional en sus cuatro sedes: Claustro la Encarnación, Casa Obando, Edificio Bicentenario y Sede Norte.

3. DEFINICIONES

RIESGOS 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.

RIESGOS DE SEGURIDAD DIGITAL: Combinación de amenazas y vulnerabilidades en el entorno digital. Incluye aspectos relacionadas con el ambiente físico, digital y las personas.

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.

Es necesario que en la descripción del riesgo concurran los componentes de su definición: acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado.

RIESGOS INHERENTES: Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar la probabilidad o su impacto.

RIESGOS RESIDUALES: Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.

PROBABILIDAD: Posibilidad de ocurrencia de un riesgo con sus respectivos efectos, esta puede ser medida con criterios de Frecuencia, si se ha materializado (por ejemplo: número de veces en un tiempo determinado), o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado.

IMPACTO: Grado o magnitud del efecto/ materialización producido o desarrollado como consecuencia de la materialización de un riesgo.

CONSECUENCIA: Efectos generados por la ocurrencia de un riesgo que afecta los objetivos o un proceso de la entidad, sus grupos de valor y demás partes interesadas.

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.

CAUSAS DE LOS RIESGOS (FACTORES INTERNOS O EXTERNOS): son los medios, las circunstancias que originan los riesgos, entendidos todos los sujetos u objetos que tienen la capacidad de originar un 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 las entidades.

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL: Esta hace referencia al propósito y lineamientos de la Alta Dirección, para gestionar, administrar y mitigar la posibilidad de ocurrencia de los riesgos de gestión y corrupción en la Institución.

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.

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

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

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

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

INTEGRIDAD: Propiedad de exactitud y completitud.

DISPONIBILIDAD: propiedad de ser accesible y utilizable a demanda por una entidad.

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.

APETITO AL RIESGO: Magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

4. DOCUMENTOS Y REGISTROS:

Los documentos y registros utilizados en el procedimiento se relacionan a continuación:

DOCUMENTOS Y REGISTROS	CÓDIGO
Manual de usuario Riesgos	No Aplica
Aplicativo de Riesgos dispuesto en SGI	No Aplica

5. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

El Colegio Mayor del Cauca, tiene como compromiso realizar la administración de los posibles riesgos de gestión, riesgos de corrupción y seguridad digital que se puedan presentar en la Institución; donde la alta dirección, los líderes de proceso y sus equipos de trabajo, de manera oportuna deberán identificar, evaluar, gestionar y minimizar aquellos eventos que generen posibles impactos negativos en la gestión; además, asegurar el manejo eficiente y eficaz de los recursos destinados para ello; con el fin de garantizar el cumplimiento de los objetivos y metas definidos en la planificación institucional con enfoque en riesgos y oportunidades, y que contribuyan a la adecuada toma de decisiones.

Para la adecuada gestión de los riesgos enmarcados en la anterior política, la institución aplicará como metodología la emitida por el Departamento Administrativo de la Función Pública.

6. DESARROLLO

6.1 IDENTIFICACIÓN DE RIESGOS

Los líderes de proceso identificarán y establecerán los controles, periodicidad y responsabilidades en la mitigación de riesgos, aplicando la siguiente metodología dispuesta en el aplicativo de riesgos plataforma SGI:

6.1.1 Conocimiento y análisis de la entidad

Para analizar el contexto general de la IUCMC es necesario conocer aspectos como: Planeación Institucional, Mapa de Procesos, Cadena de valor, objetivos estratégicos, Misión, Visión, Caracterización de Procesos.

Planeación Institucional: El cumplimiento de los objetivos estratégicos institucionales presentes en la planeación institucional aprobada, se realiza mediante los procesos estratégicos, misionales, de apoyo y evaluación.

Mapa de procesos: El cual es un estándar organizacional que soporta la prestación del servicio para el cumplimiento de la misión, visión y objetivos institucionales enmarcados en su Proyecto Educativo Institucional (PEI) y el Plan de Desarrollo Institucional (PDI).

Cadena de valor: Interrelación de los procesos dirigidos a satisfacer las necesidades y requisitos de los usuarios.

Caracterización de procesos: Establece su objetivo, alcance, entradas, actividades de transformación, salidas, proveedores, clientes.

6.1.2. Contexto Estratégico.

El proceso de Planeación a través del responsable (Asesor de Planeación) proporciona a los líderes de procesos o subprocesos el contexto estratégico.

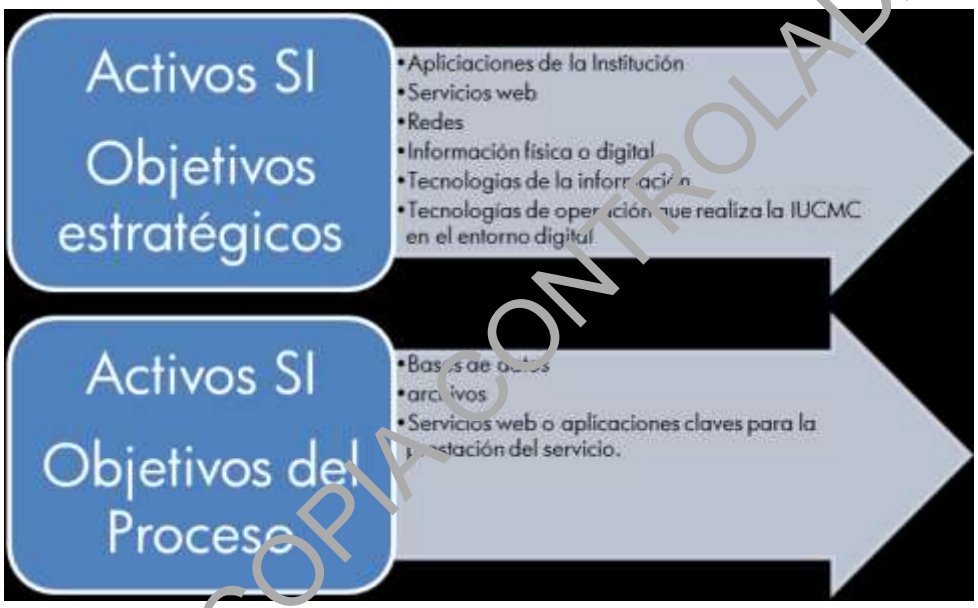
Los líderes de procesos deben realizar el análisis del contexto interno y externo de la Institución teniendo en cuenta los siguientes aspectos:

Para el análisis del contexto se pueden aplicar entrevistas estructuradas con expertos en el área de interés, reuniones con directivos y con personas de todos los niveles, evaluaciones individuales, lluvias de ideas con los servidores de la Institución, entrevistas con personas ajenas a la misma, definiendo y

contribuyendo al control de la Institución frente a la exposición al riesgo e impidiendo que esta actué en dirección contraria a los propósitos Institucionales.

6.1.3 Identificación de activos de seguridad de la información.

Un activo se define como cualquier elemento que tenga valor para la institución y el cual se debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.



6.1.4 Redacción de Riesgos

Es importante para la redacción de los riesgos realizar las siguientes preguntas:
¿Qué puede suceder? Evaluar la afectación del cumplimiento del objetivo estratégico o del proceso.
¿Cómo puede suceder? Establecer las causas a partir de los factores determinados en el contexto
¿Cuándo puede suceder? Determinar de acuerdo al desarrollo del proceso.
¿Qué consecuencias tendría su materialización? Determinar los posibles efectos de la materialización del riesgo.

En lo relacionado con los riesgos de corrupción se debe definir de la siguiente manera:
Acción u omisión + Uso del Poder + Desviación de la Gestión de lo público + el beneficio privado.

Los riesgos deberán documentarse en el aplicativo de riesgos.

6.2 VALORACIÓN DE LOS RIESGOS

6.2.1 Riesgo Inherente:

Para analizar cada riesgo se debe establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, teniendo en cuenta los criterios para calificar probabilidad e impacto, los cuales se encuentran definidos en el aplicativo de riesgos.

6.2.2 Riesgo Residual:

Se deben confrontar los resultados del análisis del riesgo inicial frente a los controles establecidos, determinando la zona de riesgo final. Ir al aplicativo de riesgos para realizar el análisis de riesgos.

6.3 EVALUACÓN DE LOS RIESGOS:

6.3.1 Riesgos antes de los controles:
Se identifican los riesgos inherentes o subyacentes que pueden afectar el cumplimiento de los objetivos estratégicos y de proceso

6.3.2 Causas Fallas:
Se identifican las causas o fallas que pueden dar origen a la materialización del riesgo.

6.3.3 Controles:

Para cada causa se identifica el control o controles; cuando el control sirva para atacar varias causas se debe repetir el control asociado de manera independiente a la causa específica.

Para establecer el control se deben tener en cuenta los siguientes pasos:
Paso 1. Definir responsable de llevar a cabo la actividad del control
Paso 2. Definir periodicidad definida para su ejecución
Paso 3. Establecer el propósito del control
Paso 4. Establecer cómo se realiza la actividad del control
Paso 5. Indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.
Paso 6. Dejar evidencia de la ejecución del control

6.3.4 Riesgos después de los controles:
Evaluar si los controles están bien diseñados para mitigar el riesgo y si estos se ejecutan como fueron diseñados.

6.4 VALORACIÓN DE LOS CONTROLES:

El Asesor de Planeación como segunda línea de defensa y el Asesor de Control Interno como tercera línea de defensa valorarán los controles establecidos por los líderes de los procesos con el fin de establecer si el control está bien diseñado para mitigar el riesgo.

6.4.1 Análisis y evaluación de los controles para mitigación de los riesgos.
Se deberán realizar las siguientes preguntas ¿El control está diseñado y se ejecuta para mitigar el impacto del riesgo una vez se materialice? y ¿El control está diseñado y se ejecuta para mitigar la probabilidad de que el riesgo se materialice?

Variables a tener en cuenta en la evaluación de los controles:

6.4.2 Resultados de la evaluación del diseño

Una vez evaluadas las variables de la evaluación de controles se debe calificar el diseño y la ejecución de los controles de la siguiente manera:

Calificación del diseño		Calificación de la ejecución	
Rango	**Resultado**	**Rango**	**Resultado**
Fuerte	96 y 100	Fuerte	**Control se ejecuta de MANERA CONSISTENTE por parte del responsable**
Moderado	86 y 95	Moderado	**Control se ejecuta ALGUNAS VECES por parte del responsable**
Débil	0 y 85	Débil	**Control NO se ejecuta parte del responsable**

6.5 MAPA RESIDUAL:

Se obtiene una vez analizado y evaluado los controles para la mitigación de los riesgos.

El tratamiento a los riesgos se da en tres categorías: **Aceptar el riesgo**: no se adopta ninguna medida (Está categoría no aplica para riesgos de corrupción), **Reducir el riesgo**: Conlleva a implementar controles**, Evitar el riesgo:** No continua o no inicia la actividad que causa el riesgo, **Compartir el riesgo**: Se transfiere o se comparte el riesgo. (Para los riesgos de corrupción se pueden compartir pero no transferir su responsabilidad).

6.6 MONITOREO Y REVISIÓN:

Esta actividad da cumplimiento a la Séptima Dimensión en MIPG de Control Interno, en donde se establecen las responsabilidades y roles distribuidos de la siguiente manera:

Primera línea de defensa: Identifica, analiza, valora, realiza monitoreo y acciones de mejora relacionados con el control y gestión de riesgo. A cargo del Rector y líderes de procesos.
Segunda línea de defensa: Asegura que los controles diseñados e implementados por la primera línea de defensa funcionen de manera adecuada. A cargo de Asesor Planeación, líderes de sistemas de gestión de la entidad.
Tercera línea de defensa: Proporciona información sobre la efectividad del Sistema de Control Interno. A cargo del Asesor Control Interno.

7. DOCUMENTOS DE REFERENCIA

Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital. Versión 4. Octubre 2018. Función Pública.

Gestión del Riesgo de Corrupción, Ley 1474 de 2011 Estatuto Anticorrupción Art. 73

Manual Operativo Sistema de Gestión MIPG. Modelo Integrado de planeación y Gestión – Séptima Dimensión Control Interno

Guía para la Gestión de Riesgo de Corrupción 2015, Presidencia de la Republica.

Decreto 648 de 2017

8. CONSIDERACIONES GENERALES

8.1 Roles y Responsabilidades frente a la Administración del Riesgo.

8.1.1 Rol de la línea estratégica en el monitoreo y revisión de los riesgos y actividades de control.

La alta dirección y el equipo directivo, a través de sus comités deben monitorear y revisar el cumplimiento a los objetivos a través de una adecuada gestión de riesgos con relación a lo siguiente:

- Revisar los cambios en el Direccionamiento Estratégico y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados.
- Revisar el adecuado desdoblamiento de los objetivos institucionales a los objetivos de procesos, que han servido de base para llevar a cabo la identificación de los riesgos.
- Hacer seguimiento en el Comité Institucional y de Control Interno a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna.
- Revisar el cumplimiento a los objetivos institucionales y de procesos y sus indicadores e identificar en cado de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.
- Hacer seguimiento y pronunciarse por lo menos cada trimestre sobre el perfil de riesgo inherente y residual de la entidad, incluyendo los riesgos de corrupción y de acuerdo a las políticas de tolerancias establecidas y aprobadas.
- Revisar los informes presentados por lo menos cada trimestre de los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos.

- Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento.

8.1.2 Rol de la primera línea de defensa.

Los gerentes públicos y los líderes de proceso deben monitorear y revisar el cumplimiento de los objetivos institucionales y de sus procesos a través de una adecuada gestión de riesgos, incluyendo los riesgos de corrupción con relación a lo siguiente:

- Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos, para la actualización de la matriz de riesgos de su proceso.
- Revisar como parte de sus procedimientos de supervisión, la revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos.
- Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos.
- Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.
- Revisar y reportar a planeación, los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y las metas, a través del análisis de indicadores asociados a dichos objetivos.
- Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento a los objetivos.
- Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de los riesgos.

8.1.3 Rol de la segunda línea de defensa.

Los gerentes públicos y líderes de proceso deben monitorear y revisar el cumplimiento de los objetivos institucionales y de sus procesos a través de una adecuada gestión de riesgos, incluyendo los riesgos de corrupción con relación a lo siguiente:

- Revisar los cambios en el Direccionamiento Estratégico o en el entorno y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar y apoyar en la actualización de las matrices de riesgos.
- Revisar la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos, que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.
- Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos.
- Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que esté por fuera del perfil de riesgo de la entidad.
- Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos.
- Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos.

8.1.4 Rol de la tercera línea de defensa.

La oficina de Control Interno o Auditoría Interna monitorea y revisa de manera independiente y objetiva el cumplimiento de los objetivos institucionales y de procesos, a través de la adecuada gestión de riesgos, incluyendo los riesgos de corrupción con relación a lo siguiente:

- Revisar los cambios en el Direccionamiento Estratégico o en el entorno y cómo estos puedan generar nuevos riesgos o modificar lo que ya se tienen identificados en cada uno de los procesos, con el fin de que se

identifiquen y actualicen las matrices de riesgos por parte de los responsables.

- Revisar la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos, que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.
- Revisar que se han identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, incluyendo los riesgos de corrupción.
- Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la Primera Línea de Defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos.
- Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que esté por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas.
- Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos y los planes de acción establecidos como resultado de las auditorías realizadas, se realicen de manera oportuna, cerrando las causas raíz del problema, evitando en lo posible la repetición de hallazgos o materialización de riesgos.

8. ANEXOS

Aplicativo y manual de Riesgos – plataforma SGI

9. CONTROL DE CAMBIOS

FECHA DE CAMBIO	CAMBIO REALIZADO
2 de junio de 2021	Se actualiza código de procedimiento según nueva TRD. Se establece como una política.
1 de noviembre de 2019	Actualización del procedimiento según las actividades y definiciones descritas en la Guía de Administración del

	Riesgo 2018.
14 de marzo de 2019	Se actualiza los responsables de elaboración y revisión del procedimiento. Se actualiza la Guía de Administración del Riesgo 2018. Se actualiza el ítem de Análisis del Riesgo y su valoración. Se actualiza la actividad de Monitoreo de los riesgos y sus responsables. Se actualiza el punto de Consideraciones Generales según los roles de la Guía de Administración del Riesgo 2018.
11 de septiembre de 2018	Se eliminan del punto 7.1.2, como responsabilidades del representante de la dirección: -Dirigir y coordinar las actividades del Equipo MECI. -Coordinar con los directivos o responsables de cada proceso las actividades que requiere realizar el Equipo MECI, en armonía y colaboración con los servidores de dichas áreas. Se eliminan responsabilidades 7.1.3. Equipo MECI: Apoyar el proceso de implementación y fortalecimiento continuo del Modelo bajo las orientaciones del representante de la dirección. Capacitar a los servidores de la entidad en el Modelo e informar los avances en la implementación y fortalecimiento continuo del mismo. Asesorar a los procesos de la institución en la implementación y fortalecimiento continuo del Modelo. Trabajar en coordinación con los servidores designados por los otros procesos en aquellas actividades requeridas para la implementación y fortalecimiento continuo del Modelo. Revisar, analizar y consolidar la información para presentar propuestas para la implementación y fortalecimiento continúo del Modelo al representante de la dirección, para su aplicación. Realizar seguimiento a las acciones de implementación y

	fortalecimiento continúo e informar los resultados al representante de la dirección, para la toma de decisiones.
Agosto 17 de 2017	1. OBJETIVO. Se articuló en el objetivo los riesgos de gestión y riesgos de corrupción. 3. DEFINICIONES. Se adicionó al punto de definiciones, los siguientes elementos y sus significados: Consecuencia, Corrupción, Gestión del riesgo de corrupción y Riesgo de corrupción. Se modificó en el mismo punto, en el significado de impacto, la palabra aparición por materialización. Se suprimió en la definición de mapa de riesgos las palabras: resumen, mapa inherente y mapa residual; para así integrar en la definición los riesgos de corrupción. Se modificó Política de Administración del Riesgo, integrando en esta los riesgos de gestión y riesgos de corrupción. Se realizó ajustes a la redacción. Se realizó ajustes a la redacción, se determinaron los periodos de monitoreo y seguimiento según su grado de exposición y se adiciono el cronograma de seguimiento a los riegos de corrupción. Se incorporó normatividad vigente como: Ley 1474 de 2011, Decreto 943 de 2014 MECI- 2014 y Guía para la Gestión de Riesgo de Corrupción 2015 y Decreto 648 de 2017. Se actualizaron los roles y responsabilidades frente a la Administración del Riesgo, según lo dispuesto en la normatividad aplicable.

	Se elimina el documento de hoja de trabajo para la administración de los riesgos. No es un registro.
Septiembre 29 de 2016	Se actualizó el procedimiento de Administración de Riesgo según la nueva estructura del MECI-2014, bajo las disposiciones del Decreto 943. - Se modificó el Alcance del procedimiento de acuerdo a la nueva estructura del MECI-2014. - Se adicionó un elemento a la definición de Causas de los Riesgos. - Se adicionó elementos de medición junto a ejemplos en la definición de Probabilidad. - Se adicionaron directrices en el Contexto Estratégico y en la Identificación del Riesgo. - Se modificó en Identificación del Riesgo - el cual es subido al Aplicativo de Administración de Riesgos, en el cual se registran. - Se modificó el Análisis y Valoración del Riesgo en cuanto, el cual es realizado en el Aplicativo de Administración de Riesgos y se califica el riesgo. - Se modificó y aclaró el Monitoreo de los Riesgos; el monitoreo y seguimiento de los riesgos establecidos, como el de sus controles y la ejecución de las acciones de tratamiento debe estar a cargo de los responsables de los procesos y el seguimiento de verificación de ejecución de las mismas por parte del Asesor de Control Interno. Se eliminaron los nombres de quien elabora, revisa y aprueba el procedimiento. Solo se coloca el cargo. Se incluyó como documento de referencia el aplicativo de Administración de riesgos.
Junio 2011	Título: Administración del Riesgo Definiciones: se adicionó mapa inherente, mapa residual y riesgo residual. Item 5. Desarrollo Se ajustaron responsables de las actividades del procedimiento: Asesor Planeación, Líderes de proceso, Asesor Control Interno.

	Item 7. Consideraciones Generales Se ajustaron los roles y responsabilidades de Representante de la dirección, Equipo directivo y operativo y Asesor de control interno.