CONTENIDO

1. POLITICA DE ADMINISTRACIÓN DE RIESGOS 3
2. OBJETIVO 3
3. ALCANCE 3
4. RESPONSABLES 3
5. TERMINOS Y DEFINICIONES 5
6. NORMATIVIDAD LEGAL Y APLICABLE 8
7. GENERALIDADES 9
8. CONTEXTO INSTITUCIONAL 10
9. ETAPAS PARA LA ADMINISTRACIÓN DE RIESGOS 11
9.1 IDENTIFICACIÓN DEL RIESGO 12
9.1.1 Descripción del riesgo 13
9.1.2 Factores de riesgo 14
9.1.3 Causas del riesgo 15
9.1.4 Consecuencias del riesgo 15
9.1.5 Descripción de la Posible Materialización del Riesgo 16
9.1.6 Concepto Integral del Riesgo 16
9.1.7 Clasificación de los riesgos 17
9.2 ANALISIS DEL RIESGO 18
9.2.1 Identificación de Controles 18
9.2.2 Calificación del riesgo 19
9.2.3 Evaluación del riesgo 21
9.3 VALORACIÓN DEL RIESGO 22
9.3.1 Tipos de controles 23
9.3.2 Evaluación de los controles 24
9.3.3 Evaluación riesgo residual 25

9.4 INTERVENCIÓN 26
9.4.1 Opciones de Manejo y acciones de tratamiento del riesgo 26
9.4.2 Actividades de contingencia 27
9.5 MONITOREO Y EVALUACIÓN 28
9.5.1 Materialización del Riesgo 29
9.5.2 Evaluación Independiente 30
10. MAPA DE RIESGOS 30
10.1 Mapa de riesgos institucionales 31
10.2 Mapa de riesgos de corrupción 31
10.3 Mapa de riesgos operativos 31
10.4 Mapa de riesgos consolidado 31
12. ANEXOS 35
13. CONTROL DE CAMBIOS 35

Revisó	Aprobó
GERENTE DE PLANEACIÓN ESTRATÉGICA Y PROYECTOS	COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO
30/07/2019	30/07/2019

1. POLITICA DE ADMINISTRACIÓN DE RIESGOS

Todo proceso de gestión incorpora situaciones o eventos que pueden generar desviaciones en la consecución de sus objetivos, por lo anterior, CISA, a través de sus líneas de defensa, se compromete a diseñar herramientas que permitan reducir la probabilidad o mitigar el impacto de la materialización de los riesgos, para lo cual, implementará y fortalecerá las etapas de administración del riesgo mediante actividades de prevención, sensibilización y control para el buen funcionamiento de la Entidad y el cumplimiento de los objetivos institucionales.

Considerando lo anterior, a través de la presente circular se desarrollan cada una de las etapas, las cuales contienen entre otros el nivel de aceptación al riesgo, niveles para calificar el impacto, tratamiento del riesgo, periodicidad y niveles de responsabilidad para el seguimiento.

2. OBJETIVO

Definir una metodología para la administración del riesgo orientada a minimizar su ocurrencia y mitigar su impacto ante una eventual materialización, buscando la consecución de sus objetivos institucionales.

3. ALCANCE

Esta Política contempla los riesgos estratégicos, financieros, operativos, de corrupción y de seguridad digital. No contempla los riesgos asociados a Sistema de Seguridad en el Trabajo, Gestión Ambiental y Gestión de Proyectos toda vez que se tratan en las normativas correspondientes.

4. RESPONSABLES

Las responsabilidades sobre la administración de riesgos en la entidad se conforman de la siguiente manera:

LÍNEA ESTRATÉGICA - ALTA DIRECCIÓN:

- ✓ Revisar y analizar las propuestas presentadas por la Gerencia de Planeación Estratégica y Proyectos para la Política de Administración del Riesgo y formalizarlas para su implementación en la Entidad.
- ✓ Promover la administración de riesgos como un componente fundamental dentro de la operación de la Entidad.
- ✓ Realizar seguimiento periódico al cumplimiento de la política de administración de riesgos definiendo acciones de mejora ante posibles desviaciones.

PRIMERA LÍNEA DE DEFENSA - LÍDERES DE PROCESO Y EQUIPO OPERATIVO:

- ✓ Establecer y revisar el contexto institucional (interno y externo), así como de definir las partes interesadas para su proceso.
- ✓ Identificar, analizar, evaluar y valorar los riesgos del proceso a través del anexo "Ficha Técnica de Riesgos".
- ✓ Realizar el monitoreo a los riesgos del proceso a través del Aplicativo de Seguimiento a la Estrategia (ASE).
- ✓ Garantizar que la construcción de los riesgos asociados al proceso fue un proceso participativo.
- ✓ Divulgar a todos los colaboradores a cargo, el mapa de riesgos operativo y de corrupción de proceso.
- ✓ Garantizar la ejecución de los controles, su correcta documentación y aplicación y la implementación de las acciones de tratamiento y fortalecimiento de los controles
- ✓ Realizar seguimiento periódico al comportamiento de los riesgos y, en caso de su eventual materialización, implementar las actividades de contingencia diseñadas y reportar a la Gerencia de Planeación Estratégica y Proyectos.
- ✓ El equipo operativo debe servir de enlace directo entre el proceso y la Gerencia de Planeación Estratégica y Proyectos para garantizar la aplicación de las metodologías desarrolladas.

SEGUNDA LÍNEA DE DEFENSA - GERENCIA DE PLANEACIÓN ESTRATÉGICA Y PROYECTOS:

- ✓ Generar propuestas sobre la metodología y políticas para la administración del riesgo de la Entidad y presentarlas para aprobación del Comité de Coordinación de Control Interno.
- ✓ Coordinar, liderar, capacitar y asesorar en la aplicación de la metodología y políticas desarrolladas.
- ✓ Realizar un monitoreo independiente al cumplimiento de las etapas para la administración de riesgos.
- ✓ Consolidar el mapa de riesgos institucional y socializarlo a las partes interesadas.
- ✓ Cargar en el Aplicativo de Seguimiento a la Estrategia (ASE) los riesgos identificados.

TERCERA LÍNEA DE DEFENSA - AUDITORÍA INTERNA:

- ✓ Asesorar en metodologías para la identificación y administración de los riesgos, en coordinación con la segunda línea de defensa.
- ✓ Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos claves de la entidad
- ✓ Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos
- ✓ Alertar sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas
- ✓ Realizar seguimiento a las acciones establecidas en los planes de tratamiento.

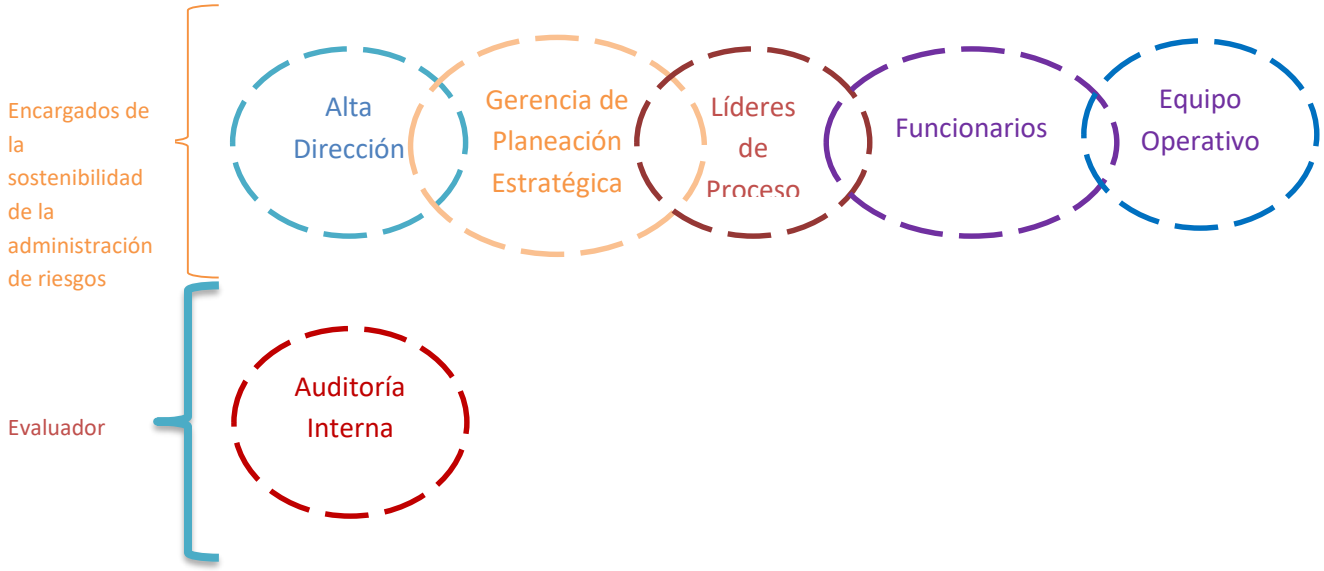
FUNCIONARIOS:

- ✓ Ejecutar los controles y acciones definidas para la administración de los riesgos identificados.

- ✓ Aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad.

EQUIPO OPERATIVO:

- ✓ Participar tanto en la actualización como en la implementación y fortalecimiento continuo de la Política de Administración de Riesgos



5. TERMINOS Y DEFINICIONES

Acciones asociadas	Acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar compartir o transferir) orientadas a fortalecer los controles identificados. Se deben formular acciones cuando se han identificado fallas en los controles y posterior a su calificación.
Administración de riesgos	Conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.
Amenaza	Situación externa que no controla la entidad y que puede afectar su operación.
Análisis del riesgo	Etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo, de acuerdo con la frecuencia de ocurrencia y el nivel de impacto definido.
Asumir el riesgo	Opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa. En la entidad, asumir el

	riesgo considera la necesidad de seguir aplicando los controles identificados, aunque no es necesario generar planes de tratamiento.
Calificación del riesgo	Estimación independiente de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
Causa	Medios, circunstancias y/o agentes que generan riesgos.
Compartir o transferir el riesgo	Opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsorcing, seguros, sitios alternos.
Consecuencia	Efecto que se puede presentar cuando un riesgo se materializa.
Contingencias	Conjunto de acciones inmediatas y responsables para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio.
Control	Acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.
Control correctivo	Acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.
Control preventivo	Acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.
Debilidad	Situación interna que la entidad puede controlar y que puede afectar su operación.
Evaluación del riesgo	Resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.
Evitar el riesgo	Opción de manejo donde se deben encaminan las acciones a prevenir la materialización del riesgo, por ejemplo mediante rediseño o eliminación de procesos.
Factores de Riesgos	Son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.
Formato levantamiento de riesgos	Herramienta de la Entidad que contempla las orientaciones para ejecutar cada una de las etapas de administración del riesgo.
Frecuencia	Ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.

Identificación del riesgo	Etapa de la administración del riesgo, donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con las clases de riesgo definidos. La identificación del riesgo implica la identificación de las fuentes de riesgo, los eventos, sus causas y sus consecuencias potenciales.
Impacto	Medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.
Información general del riesgo	Etapa de administración donde se define la información general del riesgo: proceso, tipo de riesgos, responsable y responsable operativo.
Mapa de riesgos	Documento que de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.
Materialización del riesgo	Ocurrencia del riesgo identificado.
Monitoreo del riesgo	Verificación, supervisión, observación crítica o determinación continúa del estado del riesgo con el fin de identificar cambios del nivel de desempeño requerido o esperado de cada una de las etapas de administración, así como el nivel de cumplimiento y efectividad de los controles y acciones definidas.
Opciones de manejo	Posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).
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. En este plan, se deben definir las acciones anuales que la Entidad considere pertinentes para garantizar una adecuada administración de riesgos de corrupción.
Política de Administración del Riesgo	Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.
Probabilidad	Medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.
Procedimiento	Conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.
Proceso	Conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asignan recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.

Reducir el riesgo	Opción de manejo que determina la formulación de acciones para disminuir la probabilidad y/o el impacto del riesgo mediante la generación el fortalecimiento de controles.
Riesgo	Posibilidad de que se presente un evento que genere un impacto negativo o positivo sobre los objetivos institucionales o de un proceso.
Riesgo de corrupción	Posibilidad de que, por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.
Riesgo inherente	Evaluación inicial del riesgo, de acuerdo con la calificación de la probabilidad e impacto. Esta evaluación es resultado del análisis de las condiciones reales de administración del riesgo identificado.
Riesgo institucional	Riesgos que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen alguna de las siguientes características: Son clasificados como riesgos estratégicos. Son clasificados como riesgos de corrupción.
Riesgo residual	Nivel de riesgo que permanece luego de determinar y calificar los controles para su administración.
Valoración del Riesgo	Establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir y si es necesario, las acciones a desarrollar para el fortalecimiento de controles.

6. NORMATIVIDAD LEGAL Y APLICABLE

Normatividad	Descripción
Constitución Política de Colombia.	Artículos 209 y 269.
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.
Ley 489 de 1998	Estatuto Básico de Organización y funcionamiento de la administración pública.
ICONTEC: NTC-5254	Norma Técnica Colombiana de Gestión del Riesgo.
ICONTEC: NTC-ISO 31000	Norma Técnica Colombiana Gestión del Riesgo - Principios y Directrices.

Ley 1474 DE 2011	Normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
Decreto 019 de 2012	Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública. Regulado por el Decreto 1450 de 2012 y el Decreto 1510 de 2013
Decreto 2641 de 2012	Por el cual se reglamentan los artículos 73 y 76 de la Ley 1474 de 2011
Ley 1712 de 2014	Ley de Transparencia y de Acceso a la Información Pública Reglamentada parcialmente por el Decreto Nacional 103 de 2015
Decreto 943 de 2014	Por el cual se actualiza el Modelo Estándar de Control Interno (MECI)
Decreto 1083 de 2015	Decreto Único Reglamentario del Sector Función Pública
Decreto 124 de 2016	Por el cual se sustituye el Título 4 de la Parte 1 del Libro 2 del Decreto 1081 de 2015, relativo al "Plan Anticorrupción y de Atención al Ciudadano".
Decreto 1499 de 2017	Por el cual se modifica el decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con sistemas de gestión establecido en el artículo 133 de la Ley 1753 de 2015
Decreto 648 de 2017	Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentaria Único del Sector de la Función Pública
Decreto 612 de 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

7. GENERALIDADES

Con base en los conceptos de la guía NTC ISO 31000:2009 y los lineamientos impartidos para la Administración del Riesgo por el Departamento Administrativo de la Función Pública, se considera el riesgo como *el efecto de la incertidumbre sobre los objetivos*. *Este efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos.* Según lo anterior, CISA enfrenta factores, influencias internas y externas, que crean incertidumbre sobre si se lograrán o no los objetivos de la Organización. Es el efecto que esta incertidumbre tiene en el cumplimiento de los objetivos, lo que se denomina riesgo.

En este sentido, "la administración de riesgos es un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de tal forma que permita a la Entidad minimizar pérdidas y maximizar oportunidades".[1]

Todos los procesos de CISA están sometidos a riesgos que pueden afectar el cumplimiento de los objetivos previstos; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos. La presente Circular Normativa tiene como objetivo establecer la metodología que permita dar cumplimiento a la política de administración de riesgos y de esta manera posibilitar la mejora continua en el proceso de toma de decisiones.

8. CONTEXTO INSTITUCIONAL

Son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución. Definir el contexto institucional contribuye al control de la entidad frente a la exposición al riesgo, ya que permite conocer las situaciones generadoras de riesgos, para posteriormente considerarlas al momento de efectuar los análisis correspondientes.

Para la definición del contexto, es fundamental tener claridad de la misión institucional, sus objetivos y tener una visión sistémica de la gestión, para, a continuación, identificar los factores internos y de proceso (debilidades) y externos (amenazas) que puedan generar riesgos que afecten el cumplimiento de los objetivos institucionales.

La definición del contexto es una actividad orientadora y es la base para la identificación del riesgo, dado que su análisis suministrará información importante sobre las CAUSAS del riesgo.

El contexto institucional de CISA se revisará teniendo en cuenta los cambios administrativos que puedan afectar la operación de la entidad, la revisión se realizará mediante un ejercicio llevado a cabo por los líderes de proceso en compañía de sus equipos de trabajo, con el apoyo y direccionamiento de la Gerencia de Planeación Estratégica y Proyectos.

A continuación, se presentan los factores de riesgo internos y externos definidos actualmente en la Entidad:

Factores de Riesgo Internos	Descripción
Actividades Individuales	Estabilidad laboral, disponibilidad de personal, competencias, capacitación y estado de las condiciones relacionadas con seguridad y salud en el trabajo.
Actividades y Controles gerenciales	Estado, características y disponibilidad de los mecanismos de seguimiento y medición institucionales.

[1] norma australiana ASNZ4360 de 1999

Aspectos técnicos	Capacidad operativa y de respuesta de los funcionarios de la Entidad en el desarrollo de sus funciones y obligaciones.
Aspectos tecnológicos	Operación, disponibilidad, vigencia, pertinencia y estado de los sistemas de información y comunicación de la Entidad.
Comportamiento humano	Compromiso y comportamiento ético (principios y valores) de los trabajadores.
Económicas (por la falta de recursos)	Capacidad financiera de la Entidad y administración de los recursos disponibles.
Relaciones comerciales y legales	Relacionamiento con el cliente externo y con funcionarios del gobierno nacional.

Factores de Riesgo Externos	Descripción
Circunstancias políticas	Cambios de gobierno, legislación, planes, políticas públicas, decisiones de gobernantes.
Eventos naturales	Emisiones y residuos, cortes de energía, catástrofes naturales, desarrollo sostenible.

Factores de Riesgo del Proceso	Descripción
Diseño del proceso	Claridad en la descripción del alcance y objetivo del proceso.
Interacciones con otros procesos	Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
Transversalidad	Determinación de lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
Procedimientos asociados	Pertinencia en los procedimientos que desarrollan los procesos.
Responsable del proceso	Grado de autoridad y responsabilidad de los funcionarios frente al proceso.
Comunicación entre los procesos	Efectividad en los flujos de información determinados en la interacción de los procesos.

Cuando se identifiquen las causas del riesgo, cada una de estas debe estar asociada al factor de riesgo interno, de proceso o externo correspondiente al contexto analizado.

9. ETAPAS PARA LA ADMINISTRACIÓN DE RIESGOS

A continuación, se despliega la metodología utilizada por CISA para dar cumplimiento a la Política de administración de riesgos, la cual, se desarrolla a través de etapas; en la descripción de cada etapa se desplegarán los aspectos conceptuales y operativos que se deben tener en cuenta.

Las etapas de identificación, análisis, valoración e intervención se realizarán empleando el anexo "Ficha Técnica de Riesgos". La etapa de monitoreo se realizará a través del Aplicativo de Seguimiento a la Estrategia (ASE). Ver Capitulo 11. Instructivo para el monitoreo de riesgos en el aplicativo de seguimiento a la estrategia – ase

9.1 Identificación del riesgo

La identificación del riesgo es un ejercicio participativo, que por lo general se lleva a cabo entre los líderes de cada proceso y su equipo colaborador con el apoyo de la Gerencia de Planeación Estratégica y Proyectos, los cuales, hacen un análisis de las actividades del proceso e identifican sus posibles riesgos asociados.

Para el desarrollo de esta etapa se deben considerar los siguientes aspectos:

9.1.1 Descripción del riesgo

El riesgo está directamente ligado con los atributos de calidad definidos para los productos generados por el proceso analizado. De este modo, es fundamental identificar el riesgo de la manera adecuada, para con ello garantizar un entendimiento de todos los actores involucrados y un alcance claro del mismo.

En este orden de ideas, para describir el riesgo, es necesario realizar los siguientes pasos:

Paso		Descripción	Fuente de Información
1	Revisión del objetivo y alcance del proceso.	Determinar qué hace el proceso, para qué lo hace y cómo lo hace. Revisar el alcance: dónde inicia y finaliza la gestión del proceso y qué actividades contempla. Los objetivos del proceso deben cumplir con las características SMART: Especifico, Medible, Alcanzable, Relevante, Con Tiempo definido. Si el objetivo no contempla estas características mínimas, debe revisarse y actualizarse antes de continuar con el proceso de identificación de riesgos. Se debe tener en cuenta que, al modificar el objetivo del proceso, esto pude impactar directamente sobre el alcance y los productos que de este se generan.	Caracterización del proceso
	Identificar las salidas del proceso.	Determinar cuáles son las salidas del proceso que se generan durante la ejecución del mismo.	
2	Determinar las características o requisitos que deben cumplir los productos y/o servicios identificados.	Identificar cuáles son los atributos o características específicas que debe tener cada uno de los productos y/o servicios generados por el proceso.	Normatividad interna, Normatividad legal aplicable, etc.
3	Revisar antecedentes del proceso.	Revisar experiencias pasadas, riesgos materializados recientemente, problemas generados en la entidad o en el proceso, informes y conceptos de expertos, informes de la Auditoría Interna y entes de control, información de riesgos materializados en otras entidades.	Informes de gestión Informes de auditoría

4	Determinar los riesgos.	Una vez listados los productos y/o servicios generados por el proceso, así como sus características, el análisis de la información de evaluaciones previas del proceso, informes de gestión y demás información, se describen los riesgos. No existe una fórmula única para la determinación del riesgo, sin embargo, en la medida de lo posible, CISA los formulará a nivel de los principales productos, considerando que el incumplimiento de sus atributos o características específicas es la materialización de este. Esto permite, un control más gerencial al momento de realizar análisis posteriores. Adicional a lo anterior, al momento de describir el riesgo, es importante evitar iniciar con palabras negativas como: "No…", "Que no…", o con palabras que denoten un factor de riesgo (causas) o la ausencia de un control tales como: "ausencia de", "falta de", "poco(a)", "escaso(a)", "insuficiente", "deficiente", "debilidades en…".	

9.1.2 Factores de riesgo

Como resultado del análisis del contexto institucional, se establecen los factores de riesgo como insumo para determinar las posibles causas generadoras de riesgo; por esta razón, cada una de las causas generadoras del riesgo identificado, debe estar asociada al factor externo, interno o de proceso de riesgo, según corresponda. Dichos factores, son los definidos en el capítulo de análisis de contexto institucional.

9.1.3 Causas del riesgo

Las causas son los medios o circunstancias directamente relacionados con los factores internos o externos que permiten la materialización del riesgo. Se debe garantizar la coherencia entre las causas y el riesgo identificado, teniendo en cuenta que los controles estarán orientados a la eliminación o mitigación de causas asociadas al riesgo.

"Una definición inadecuada de las causas, conlleva a un tratamiento incipiente y poco efectivo de los riesgos identificados debido a una definición errada de los controles".

9.1.4 Consecuencias del riesgo

Son los efectos sobre los objetivos de los procesos y de la entidad, que se generan o pueden generarse con la materialización del riesgo; generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como:

- Daños físicos.
- Fallecimiento.
- Sanciones.
- Pérdidas económicas.
- Pérdidas de información.
- Pérdidas de bienes.
- Pérdidas de imagen, credibilidad y confianza.
- Interrupción del servicio.
- Daño ambiental.

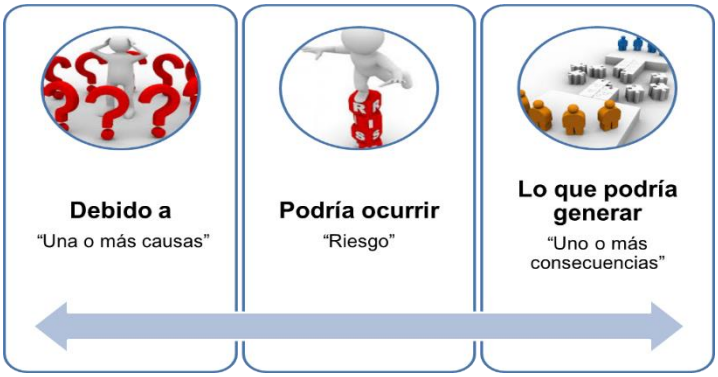
9.1.5 Descripción de la Posible Materialización del Riesgo

La Identificación del riesgo no consiste únicamente en la determinación de sus causas y consecuencias, se hace necesario, además, establecer con claridad cuando se entenderá materializado el riesgo. Esto permitirá a cualquier persona que se encargue de la gestión del mismo, considerar con precisión los aspectos que en su momento se tuvieron en cuenta. La identificación del hecho que materializará el riesgo, debe estar en completa armonía con las causas identificadas y con el riesgo mismo, realizando una descripción detallada del evento que provocará este hecho, lo que, en su momento, dará entrada a los análisis descritos en el apartado "Materialización del Riesgo".

Cabe destacar que, mediante este análisis, es posible determinar rangos de tolerancia ante los eventos de materialización. Esto permitirá centrar la atención en aspectos de importancia del riesgo y no reportar materializaciones ante hechos aislados

9.1.6 Concepto Integral del Riesgo

La identificación del riesgo no se puede realizar de manera fragmentada; debe existir una relación integral entre las causas identificadas, el riesgo y las consecuencias que podrían presentarse producto de la materialización; para evitar confusiones y definir articuladamente todos los componentes de la identificación del riesgo se establece un método apropiado que consiste en el uso del metalenguaje del riesgo para una identificación estructurada en tres partes:



El esquema anterior pretende asegurar que se identifiquen correctamente causas, riesgos y Consecuencias, sin confundir unas con otras; de no ser así, los pasos posteriores quedan viciados de error.

9.1.6.1 Aspectos a tener en cuenta para la descripción adecuada de los riesgos de corrupción

Con el fin de facilitar la identificación y correcta clasificación de los riesgos de corrupción, se sugiere tener en cuenta las siguientes preguntas orientadoras:

- ✓ ¿Se presenta una acción u omisión?
- ✓ ¿Se hace uso del poder de manera indebida?
- ✓ ¿Se identifica desviación de la gestión pública?
- ✓ ¿Implica un beneficio particular?

Si la respuesta es afirmativa para todas las preguntas anteriores, se cataloga como riesgo de corrupción.

Con respecto a la identificación de las causas para los riesgos de corrupción, estas presentan una pequeña variante frente a los riesgos operativos. Mientras que para los riesgos operativos nos preguntamos *¿por qué?* se puede presentar la situación descrita en el riesgo, en aquellos que hacen alusión a hechos de corrupción, nos centraremos en la identificación del *¿Cómo?* puede suceder el acto de corrupción. De este modo, se atacarán las posibilidades reales que se materialice un hecho de este tipo.

9.1.7 Clasificación de los riesgos

Durante la etapa de identificación, se realiza la clasificación del riesgo según sus características, con el fin de orientar la formulación de un tratamiento adecuado que posibilite su mitigación mediante la definición de controles y acciones de intervención. De este modo, en CISA clasificaremos los riesgos como:

Clases de riesgo	Definición
Estratégico	Son los riesgos relacionados con el cumplimiento de los objetivos estratégicos, la definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia. En resumen, son aquellos riesgos que se asociarán directamente con el Mapa Estratégico de la Entidad.
Operativo	Relacionados con el funcionamiento y operación de la Entidad: Ejecución de procesos, estructura de la entidad, articulación entre dependencias. Dentro de esta categoría se incluirán los Riesgos Financieros (relacionados con el manejo de los recursos de la entidad: ejecución presupuestal, elaboración estados financieros, pagos, manejos de excedentes de tesorería y manejo de los bienes) y los Riesgos de Lavado de Activos y/o Financiación del Terrorismo en los procesos que aplique.
Corrupción	Posibilidad de que, por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.

9.1.7.1 Riesgos de Negocio

En clasificación de los riesgos, se deben considerar como clase especial los denominados ***Riesgos de Negocio,*** los cuales, pueden afectar la viabilidad y sostenibilidad de la empresa desde una perspectiva sistémica, visualizando la entidad como un gran proceso.

En el siguiente cuadro, se presenta el riesgo de negocio de CISA con sus principales causas y consecuencias, destacándose, que la gestión que realiza CISA de sus riesgos estratégicos, operativos y de corrupción, buscan garantizar la mitigación de estos ***Riesgos de Negocio.***

Riesgo	Causa	Consecuencia
No viabilidad financiera de la Entidad	Insuficiente generación de inventario	Cierre de la Entidad
	Pago excesivo por los activos adquiridos	Generación de Pérdidas
	Insuficiente recaudo la cartera	Imposibilidad de atender obligaciones
	Lenta movilización de inmuebles	Pérdida de imagen y posicionamiento
	Estructuración y/o ejecución de nuevas líneas de negocio que no alcanzan la rentabilidad esperada	
	Incremento Excesivo del Gasto	

9.2 Análisis del riesgo

La etapa de análisis busca establecer para cada riesgo, su probabilidad de ocurrencia y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información cuantitativa y cualitativa para establecer el nivel de riesgo. De igual manera, se identifican los posibles controles aplicados al riesgo sin profundizar en su análisis y evaluación.

Se han establecido dos aspectos a tener en cuenta en el análisis de los riesgos identificados: La Probabilidad y el Impacto. Por la primera se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida a partir de la determinación de la frecuencia de ocurrencia del riesgo; por Impacto, se entiende las consecuencias que puede ocasionar a la Entidad la materialización del riesgo.

9.2.1 Identificación de Controles

Los controles son las acciones orientadas a minimizar la probabilidad de ocurrencia o el impacto del riesgo; estos deben estar directamente relacionados con las causas o las consecuencias identificadas y eliminarlas o mitigarlas. La administración del riesgo contribuirá a la gestión de la entidad, en la medida en que los controles se identifiquen, documenten, apliquen y sean efectivos para prevenir o mitigar los riesgos.

Es de este modo, que previo a la determinación de la probabilidad e impacto del riesgo, se deben listar los controles existentes para administrar el riesgo identificado; este ejercicio permite conocer con qué mecanismos se cuenta para controlar el riesgo y orientar una adecuada calificación, acorde con las

condiciones reales de operación. En esta etapa solo se deben listar los controles; posteriormente se realizará la descripción detallada de cada uno de estos.

El listado de los controles nace de los diferentes documentos con los que cuenta el proceso. Es por eso, que en esta fase, se deben identificar dichos documentos y transcribir los controles que apliquen para el riesgo. Cuando se identifiquen controles que no estén debidamente documentados en el proceso, se listarán de igual manera y su formulación, evaluación y formalización harán parte del plan de tratamiento de riesgos, descrito con posterioridad en este documento.

9.2.2 Calificación del riesgo

Se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar su materialización. La primera representa el número de veces que el riesgo se ha presentado en un determinado tiempo, y la segunda se refiere a la magnitud de sus efectos. Para la determinación de la calificación del riesgo, con base en la probabilidad y el impacto CISA define las siguientes tablas de calificación:

TABLA DE CLASIFICACIÓN DE LA PROBABILIDAD:

Nivel	Descriptor	Frecuencia
1	Rara vez	No se ha presentado en los últimos 24 meses
2	Improbable	Al menos una vez en los últimos 16 meses
3	Posible	Al menos una vez en los últimos 12 meses
4	Probable	Al menos una vez en los últimos 8 meses
5	Casi Seguro	Al menos una vez en los últimos 4 meses

TABLA DE CLASIFICACIÓN DEL IMPACTO:

Para la clasificación del impacto, es importante considerar los siguientes tipos de efecto con su correspondiente descripción, los cuales, podrán ser encontrados en la matriz a continuación, con su calificación correspondiente.

Tipo de impacto	Definición
Estratégico	Afecta el cumplimiento de los objetivos estratégicos. Impacto asociado a los riesgos clasificados como estratégicos.
Operativo	Afecta el funcionamiento y operación de la Entidad.
Cumplimiento	Afecta el cumplimiento de requisitos legales, contractuales, ética pública y compromiso con la comunidad.
Financieros	Afecta la disponibilidad de recursos monetarios de la Entidad para el cumplimiento de su misión.
Imagen	Afectan la credibilidad, confianza y percepción de los usuarios de la entidad.
Tecnológico	Afecta la capacidad tecnológica disponible para satisfacer las necesidades actuales y futuras y el cumplimiento de la misión.

Para identificar el impacto, ubique en la matriz, cada una de las consecuencias identificadas previamente, en la columna correspondiente al tipo de efecto (estratégico, operativo, financiero, cumplimiento, etc). Con todas las consecuencias identificadas en la matriz, seleccione como nivel de impacto, el que represente el mayor valor.

Nivel							
INSIGNIFICANTE	Afecta el cumplimiento de algunas actividades del planes de acción	Genera Reprocesos sin impacto en el producto final	Afecta el presupuesto de ingresos en un valor menor al 1%	Genera una observación u oportunidad de mejora	Afecta a una persona o una actividad del proceso.	Afecta a una persona o una actividad del proceso.	
MENOR	Afecta el cumplimiento de los proyectos estratégicos	Genera Reprocesos con impacto en el producto final	Afecta el presupuesto de ingresos en un valor entre el 1% y 5%	Genera un requerimiento	Afecta el proceso	Afecta a un grupo de servidores del proceso	
MODERADO	Afecta el cumplimiento de los objetivos estratégicos de CISA	Genera productos y/o servicios no conformes	Afecta el presupuesto de ingresos en un valor entre el 5% y 20%	Genera investigaciones disciplinarias, y/o fiscales y/o penales	Afecta varios procesos de CISA	Afecta a todos los servidores del proceso	Entre 1 y 5 preguntas afirmativas
MAYOR	Afecta el cumplimiento de la misión de CISA	Genera intermitencia en los procesos o servicios	Afecta el presupuesto de ingresos en un valor entre el 20% y 50%	Genera sanciones para la entidad	Afecta a todo CISA	Afecta a todos los servidores de CISA	Entre 6 y 11 preguntas afirmativas
CATASTRÓFICO	Afecta el cumplimiento de las metas nacionales	Genera paro total del proceso y/o de CISA	Afecta el presupuesto de ingresos en un valor mayor al 50%	Genera interrupciones en la prestación del bien o servicio	Afecta a parte interesadas de CISA	Afecta a la Nación	Entre 12 y 19 preguntas afirmativas

**La evaluación del impacto del riesgo de corrupción se realiza con base en las siguientes preguntas y el número de respuestas positivas permitirá ubicar el resultado en la matriz.*

No	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 la 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 a la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?		
9	¿Generar pérdida de información de la Entidad?		
10	¿Generar intervención de 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	¿Genera daño ambiental?		

9.2.3 Evaluación del riesgo

Permite comparar los resultados de la calificación, con los criterios definidos para establecer el grado de exposición al riesgo; de esta forma, se define la zona de ubicación del riesgo. Para ello, basta cruzar el resultado obtenido en la probabilidad y el impacto y ubicarlo en la zona correspondiente.

Se utilizará una sola matriz para efectuar la calificación de los diferentes tipos de riesgo, buscando la simplificación de la metodología, pero sin perder en ningún momento lo estricto de la evaluación en cada caso.

MATRIZ DE EVALUACIÓN DEL RIESGO

PROBABILIDAD	IMPACTO				
	Insignificante	Menor	Moderado	Mayor	Catastrófico
Casi Seguro	A	A	E	E	E
Probable	M	A	A	E	E
Posible	B	M	A	E	E
Improbable	B	B	M	A	E
Rara vez	B	B	M	A	E

Raro	Zona de Riesgo
B	Zona de Riesgo Baja
M	Zona de Riesgo Moderada
A	Zona de Riesgo Alta
E	Zona de Riesgo Extrema

9.3 Valoración del riesgo

Es la etapa en la cual se realiza la descripción y calificación de los controles asociados al riesgo e identificados en la etapa de análisis. Los controles deben estar directamente relacionados con las causas o las consecuencias identificadas para el riesgo y de este modo buscan eliminarlas o mitigarlas.

La evaluación de los controles consta de 2 fases: Diseño y Ejecución. Con la primera, se busca que los controles sean los suficientemente claros y específicos en cuanto a cómo se deberían ejecutar; con respecto a la ejecución del control, se busca que ésta se produzca de manera estandarizada por los responsables de su aplicación.

Ambas fases deben estar íntimamente relacionadas, ya que de nada sirve un control muy bien diseñado que no se ejecuta, y viceversa, un control que se ejecuta pero que no cumple con los parámetros de diseño y que puede aplicarse de maneras diferentes o por diversos responsables, tarde o temprano desembocará en la ejecución inadecuada del mismo.

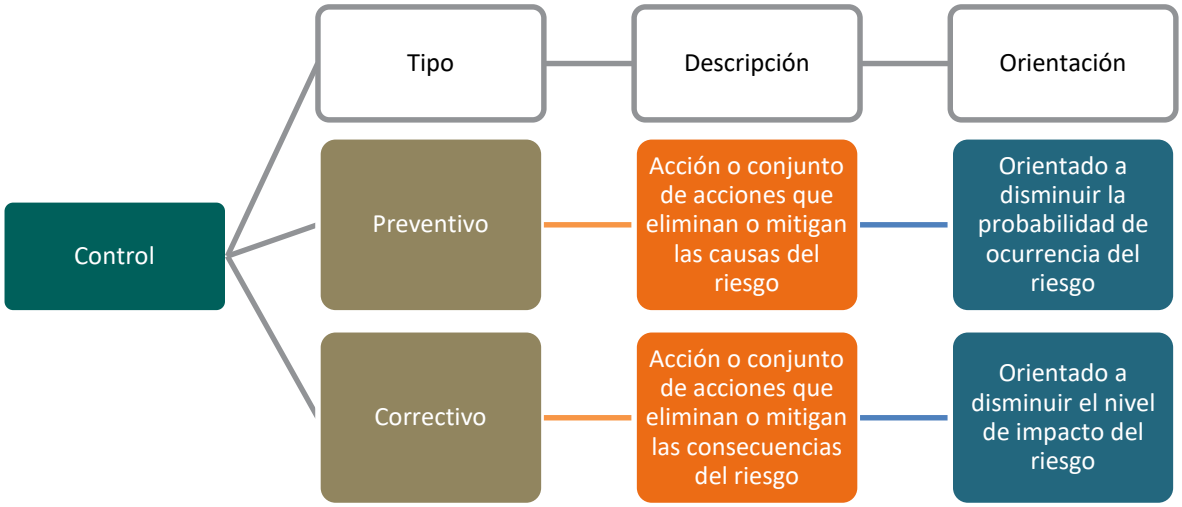
Teniendo en cuenta lo anterior, el corazón de la administración del riesgo es la aplicación de controles, los cuales, contribuirán a la gestión de la entidad, en la medida en que se identifiquen, documenten, apliquen y sean efectivos para prevenir o mitigar los riesgos.

A continuación, se presentan las características mínimas que deben tener los controles:

Característica	Descripción
Objetivos	No dependen del criterio de quien lo define y/o ejecute, sino de los resultados que se esperan obtener.
Pertinentes	Están directamente orientados a atacar las causas o consecuencias del riesgo.
Realizables	Se pueden implementar y ejecutar en la entidad.
Medibles	Permiten el establecimiento de indicadores para verificar el cumplimiento de su aplicación y/o efectividad.
Periódicos	Tienen frecuencia de aplicación en el tiempo.
Efectivos	Eliminan o mitigan las causas o consecuencias y evitan la materialización del riesgo.
Asignables	Tienen responsables definidos para su ejecución.

9.3.1 Tipos de controles

Los controles se pueden clasificar en 2 tipos:



9.3.2 Evaluación de los controles

9.3.2.1 Evaluación Individual de los controles

La evaluación individual de cada uno de los controles asociados a un riesgo se realiza con base en las fases descritas anteriormente: Diseño y Ejecución. El resultado de la evaluación es la suma de los puntajes obtenidos al responder las siguientes preguntas:

Fase	Factor	Orientación	Puntuación	
			Sí	No
Diseño	Responsabilidad	¿Existe un responsable asignado a la ejecución del control?	10	0
		¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	10	0
	Periodicidad	¿El control tiene una periodicidad definida y es la apropiada para prevenir o detectar la materialización del riesgo?	15	0
	Propósito	¿Están claramente definidas las actividades que se desarrollan para la ejecución del control y las mismas permiten verificar, validar, cotejar, comparar o revisar el propósito del control?	15	0
	Información	¿Está claramente definida la fuente de información que se utiliza para la aplicación del control siendo confiable para su aplicación?	15	0
	Aplicación	¿Se cuenta con las evidencias completas de la ejecución y seguimiento del control?	10	0
	Desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la aplicación del control son investigadas y resueltas de manera oportuna?	15	0
Ejecución	Ejecución	El control se ejecuta... De manera estandarizada por parte del responsable Algunas veces por parte del responsable Pocas veces por parte de (los) responsable (s)	10 5 0	

Los factores analizados permitirán analizar la fortaleza del control en cada una de las fases, de este modo, siempre que el puntaje del control sea menor a 96 puntos, se deberán implementar acciones orientadas a su optimización.

Ante la eventual materialización de un riesgo, se debe verificar si alguno de los controles falló o si existen causas no identificadas que provocaron este hecho, esto permitirá optimizar el control actual o formular uno nuevo que ataque la nueva causa identificada.

De igual manera, es fundamental que cada control ataque una o más causas o consecuencias de acuerdo a su naturaleza. El resultado de la evaluación individual será a su vez evaluado de manera grupal.

9.3.2.2 Calificación Grupal de los controles

Se realiza con base en el promedio de puntos obtenidos para cada uno de los controles analizados en la evaluación individual. Adicionalmente, es fundamental considerar la cobertura de las causas a través de los controles como un factor que pondera la calificación global. La totalidad de los controles deben atacar la totalidad de las causas, si no es así, se debe disminuir porcentualmente la calificación de acuerdo a la cantidad de causas descubiertas.

A manera de ejemplo, si un riesgo tiene 5 causas identificadas y se aplican 4 controles que solo atacan a 3 de las causas, se tendría.

# Control	Calificación Control Individual	Causa Atacada por el control	% de cobertura de las causas	Calificación Grupal de los controles
Control 1	80	Causa 1	60% (3 causas atacadas /5 causas identificadas)	((80+70+100+95)/4)* 60% = 51.75%
Control 2	70	Causa 2		
Control 3	100	Causa 1		
Control 4	95	Causa 3		

9.3.3 Evaluación riesgo residual

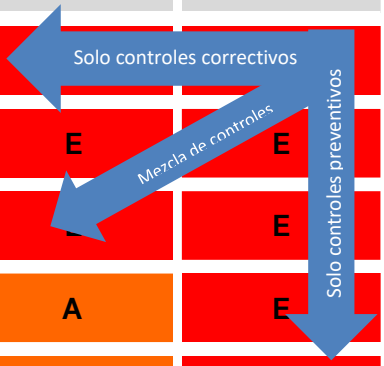
Se entiende por riesgo residual el nivel de riesgo que permanece luego de determinar y calificar los controles para su administración.

Para lo anterior, se procede la siguiente manera: Partiendo del resultado de la evaluación del riesgo (Numeral 9.2.3), y la calificación grupal de los controles, se puede modificar el riesgo de la matriz de probabilidad e impacto así:

Calificación Grupal de Controles	Movimiento Permitidos
0% – 85%	0
86% - 99%	1
100%	2

De esta manera, la matriz disminuye su posición de la siguiente forma:

PROBABILIDAD	IMPACTO				
	Insignificante	Menor	Moderado	Mayor	Catastrófico
Casi Certeza	A	A	E		
Probable	M	A	A	E	E
Moderada	B	M	A		E
Improbable	B	B	M	A	E
Raro	B	B	M	A	E



9.4 Intervención

La intervención, también conocida como etapa de manejo, se enfoca en el tratamiento que se debe dar al riesgo en el caso de identificar debilidades en los controles y adicionalmente, definir las acciones de contingencia que deberían tomarse en el caso de la materialización del riesgo.

9.4.1 Opciones de Manejo y acciones de tratamiento del riesgo

Cuando se ha determinado el riesgo residual, se debe asociar la opción de manejo mediante la cual se dará tratamiento.

Las opciones de manejo se determinan teniendo en cuenta la ubicación del riesgo según las zonas definidas así:

Raro	Zona de Riesgo	Opción de Manejo
B	Zona de Riesgo Baja	Asumir el riesgo
M	Zona de Riesgo Moderada	Reducir el riesgo
A	Zona de Riesgo Alta	Reducir el riesgo Evitar el riesgo Compartir o transferir el riesgo
E	Zona de Riesgo Extrema	Reducir el riesgo Evitar el riesgo Compartir o transferir el riesgo

Las acciones de tratamiento pueden incluir una o varias de las siguientes opciones:

- ✓ **Asumir el riesgo:** Mantener los controles existentes y realizar seguimiento periódico. En ningún caso, asumir el riesgo representará que no se ejecuten controles a los riesgos identificados. Siempre se asumirá el riesgo aplicando continuamente los controles existentes.
- ✓ **Reducir el riesgo:** Tomar medidas encaminadas a disminuir ya sea la probabilidad (medidas de prevención) o el impacto (medidas de corrección). Ej.: optimización de procesos, definición de nuevos controles, entre otros. Si el riesgo se encuentra en una zona moderada con probabilidad "rara vez" se deben mantener los controles existentes y hacer monitoreo periódico. No se hace necesario aplicar planes de tratamiento de riesgos.
- ✓ **Evitar el riesgo:** tomar las medidas encaminadas a eliminar la materialización del riesgo cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación. Ej.: cambios a la infraestructura, cambios en software, etc.
- ✓ **Compartir o transferir el riesgo:** reduce su efecto mediante el traspaso de las pérdidas a otras organizaciones, permiten distribuir una porción del riesgo con otra entidad. Ej.: seguros, sitios alternos, contratos de riesgos compartidos, etc.

Importante: Una vez identificadas las opciones de manejo se deben formular las acciones orientadas a la creación y/o fortalecimiento de los controles cuando así se requiera.

9.4.2 Actividades de contingencia

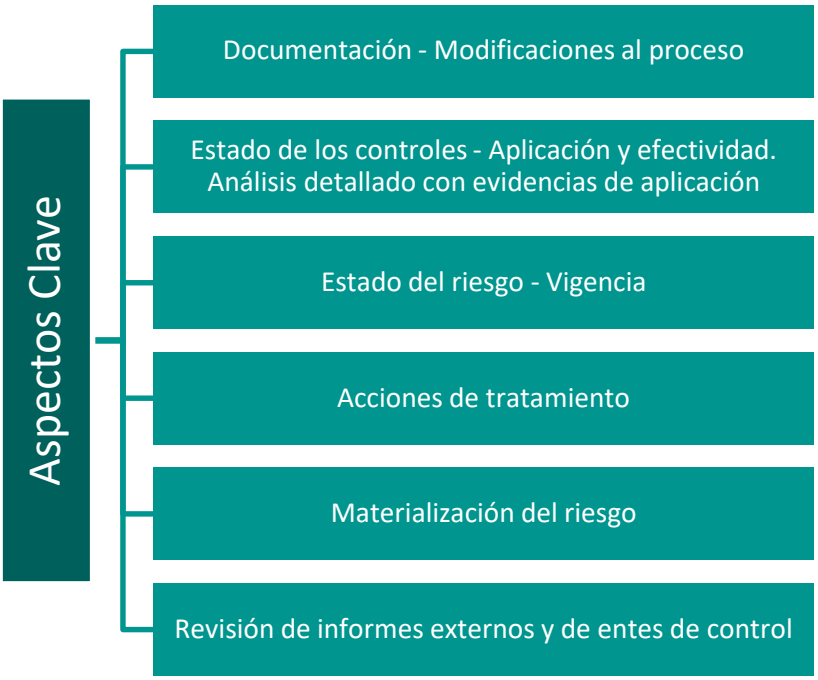
Consiste en la definición de acciones inmediatas a desarrollar en el caso de materialización del riesgo, se deben identificar **para todos los riesgos**, independiente de su evaluación residual o de los controles existentes.

Estas acciones son la respuesta inicial a la materialización del riesgo y se enfocan en las correcciones que se deben desarrollar de acuerdo con las consecuencias identificadas.

Las actividades de contingencia, permiten retornar la operación a su curso normal. Sin embargo, es necesario que posterior a su implementación, se analice la causa raíz de lo sucedido y se proyecten acciones correctivas para evitar que se vuelva a presentar el acontecimiento; dichas acciones pueden incluir la incorporación de nuevos controles al proceso o el fortalecimiento reevaluación de los existentes.

9.5 Monitoreo y evaluación

Esta etapa dinamiza la gestión integral del riesgo, cada cuatro meses (en abril, agosto y diciembre), los procesos deben realizar seguimiento al estado de sus riesgos garantizando que se analizaron entre otros los siguientes aspectos:



Con base en lo anterior, se deben responder las siguientes preguntas, las cuales orientarán las acciones a desarrollar posteriormente.

Número	Pregunta	Respuesta	Etapa a actualizar en caso de respuesta negativa
1	¿El proceso ha operado sin cambios significativos durante los últimos 4 meses?	SI/No	Identificación
2	¿El riesgo sigue siendo vigente de acuerdo a la operación del proceso?	SI/No	Identificación
3	¿Los elementos constitutivos del riesgo continúan vigentes pese a la presentación de informes internos y externos relacionados con el tema?	SI/No/N.A	Identificación
4	¿La aplicación de los controles ha resultado ser efectiva, es decir, el riesgo no se ha materializado?	SI/No	Valoración
5	¿El proceso cuenta con los soportes de la aplicación de los controles?	SI/No	Valoración
6	¿Las acciones de tratamiento se han desarrollado oportunamente?	SI/No/N.A	Manejo

Si al momento de responder las preguntas anteriores, se encuentra una respuesta negativa, es necesario actualizar los elementos del riesgo en la etapa correspondiente describiendo exactamente lo sucedido.

De igual manera, a medida que los controles son efectivos, la probabilidad deberá disminuir paulatinamente hasta lograr el nivel más bajo. En este sentido, mientras la probabilidad no se ubique en el nivel 1 “Rara vez” y los controles demuestren ser efectivos, se debe actualizar la calificación del riesgo en la matriz probabilidad e impacto de la etapa análisis del riesgo.

9.5.1 Materialización del Riesgo

La ocurrencia del riesgo o también conocida como la materialización del riesgo, es la afectación comprobada que se presenta sobre los objetivos institucionales o de proceso tras la ocurrencia de un riesgo. En este sentido, el líder de proceso debe determinar y dictaminar mediante una investigación exhaustiva, la materialización efectiva del riesgo. Es de aclarar, que el líder de proceso podrá solicitar la colaboración de las diferentes áreas institucionales a fin de garantizar la agilidad y calidad de este proceso.

Con respecto a una materialización, puede presentarse lo siguiente: No identificación del riesgo por parte del proceso y por lo tanto la no ejecución de controles para mitigarlo; la ocurrencia de una o más de las causas y que el control destinado para prevenirla no sea efectivo o que la causa de la materialización no se encuentre identificada y, por lo tanto, su control tampoco.

La identificación de la posible materialización del riesgo, es una actividad que debe tener prioridad dentro del proceso. Por lo tanto, producto de la investigación y tan pronto como se presente la materialización de un riesgo, debe realizarse el análisis correspondiente que incluya entre otras la determinación de:

- ✓ ¿Que causó la posible materialización del riesgo?

- ✓ ¿Qué control no fue efectivo para evitar la materialización del riesgo?
- ✓ ¿Qué impacto genera para el proceso o la institución la materialización de ese riesgo?
- ✓ ¿Es posible que se haya presentado en otras ocasiones sin haberlo detectado?
- ✓ ¿Qué acciones se deben realizar para reestablecer el curso de acción del proceso?
- ✓ ¿Qué actividades se deben desarrollar para fortalecer los controles?
- ✓ ¿Quiénes están implicados en la materialización del riesgo?

Cada una de estas preguntas, prepara al proceso para identificar oportunidades que le permitan fortalecer su operación y disminuir la probabilidad de ocurrencia de las causas. Por lo anterior, posterior a la ejecución de las actividades de contingencia, que permitirán retornar al proceso a su ejecución normal, es fundamental formular las acciones correctivas que fortalezcan el proceso.

A su vez, es indispensable que la alta dirección esté enterada de los sucesos acontecidos. De este modo, una vez detectada la materialización de cualquier riesgo de corrupción, operativo o de seguridad de la información, el líder de proceso deberá presentar ante el Comité de Presidencia, en un plazo no mayor a 8 días dependiendo de la gravedad de la materialización, un informe detallado, que incluya las respuestas a las preguntas antes indicadas e información adicional si lo considera pertinente y las acciones de contención o corrección que se requieran.

El Comité analizará la situación y podrá generar acciones adicionales a las ya establecidas por el proceso en el marco de la prevención de la materialización del riesgo.

También se considera fundamental, que el líder de proceso analice con el proceso Legal, en un plazo no mayor a 3 días posteriores a la materialización del riesgo, las acciones judiciales que se pueden desprender, así como las posibles reclamaciones a seguros cuando así sea procedente.

Importante: Toda materialización implica la revisión y análisis de cada una de las etapas del riesgo y afecta directamente la calificación de la probabilidad al llevarla al nivel 5 “Casi Certeza” en la matriz de riesgos.

9.5.2 Evaluación Independiente

Como parte de las responsabilidades de la tercera línea de defensa y en cumplimiento de sus actividades misionales, Auditoría interna evaluará la aplicación de la metodología y políticas definidas.

10. MAPA DE RIESGOS

El mapa de riesgos es la consolidación de la información generada a lo largo de las etapas de administración de riesgos. Dentro de esta consolidación se destacan 4 mapas fundamentales.

10.1 Mapa de riesgos institucionales

El mapa se construye con aquellos riesgos que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen alguna de las siguientes características:

- ✓ Son clasificados como riesgos estratégicos.
- ✓ Son clasificados como riesgos de corrupción.

10.2 Mapa de riesgos de corrupción

El mapa se construye con aquellos riesgos que fueron clasificados dentro de la etapa de identificación general como “Riesgos de Corrupción”.

10.3 Mapa de riesgos operativos

El mapa se construye con aquellos riesgos que fueron clasificados dentro de la etapa de identificación general como “Riesgos Operativos”.

10.4 Mapa de riesgos consolidado

Integra la totalidad de los riesgos de la Entidad.

11. INSTRUCTIVO PARA EL MONITOREO DE RIESGOS EN EL APLICATIVO DE SEGUIMIENTO A LA ESTRATEGIA – ASE

El Aplicativo de Seguimiento a la Estrategia – ASE, es el instrumento por medio del cual, la Primera Línea de Defensa, realizará la gestión administrativa permanente a los riesgos de los procesos. Este instrumento, se convierte entonces, en el repositorio oficial de información relacionada con los riesgos operativos y de corrupción que la Entidad ha identificado de acuerdo a la metodología establecida.

Considerando lo anterior, el documento “Anexo Manual - 004 Guía para la Administración del Aplicativo de Seguimiento a la Estrategia – ASE” del Manual 012 de 2018, desarrolla las principales características del Módulo de Riesgos, frente a la administración y uso de sus principales componentes.

No obstante lo anterior, en el presente documento se hará una explicación detallada del procedimiento para realizar el Monitoreo en el sistema, como parte fundamental de la gestión permanente a los riesgos.

Cabe destacar, que la gestión de los riesgos para efectos del sistema, estará a cargo del líder de proceso y del enlace operativo del proceso, los cuales, serán los encargados de desarrollar las responsabilidades

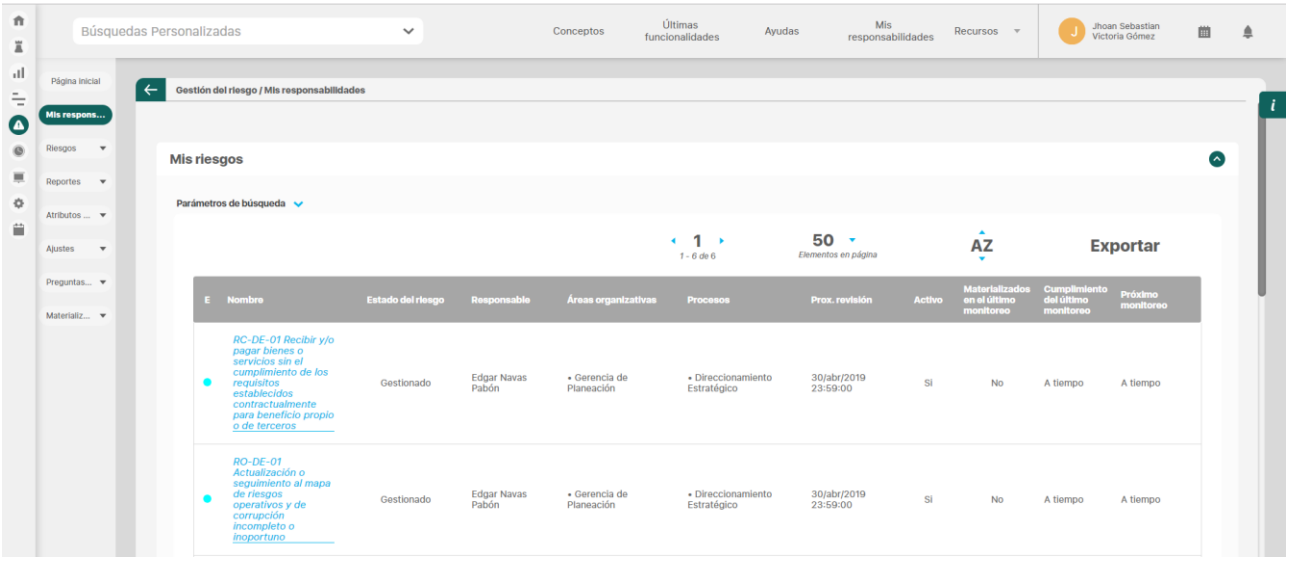
asignadas en la guía antes mencionada y los pasos que a continuación se describen para el Monitoreo de los Riesgos.

1. Ingreso al ASE

- El ingreso al sistema se realiza a través de la siguiente ruta: http://ase.cisa.gov.co/sve/ utilizando el dominio “cisa.gov.co”.
- El usuario debe identificarse con el usuario y contraseña que utiliza para el ingreso a la sesión de su computador.

2. Ubicación del Riesgo a Monitorear

- De clic en el Módulo “Gestión del Riesgo” (al lado izquierdo de su pantalla).
- De clic en el botón “Mis Responsabilidades” del menú desplegado en el paso anterior.
- En la sección “Mis Riesgos” desplegada luego del paso anterior, identifique del listado generado el riesgo al cual desea realizarle el Monitoreo.

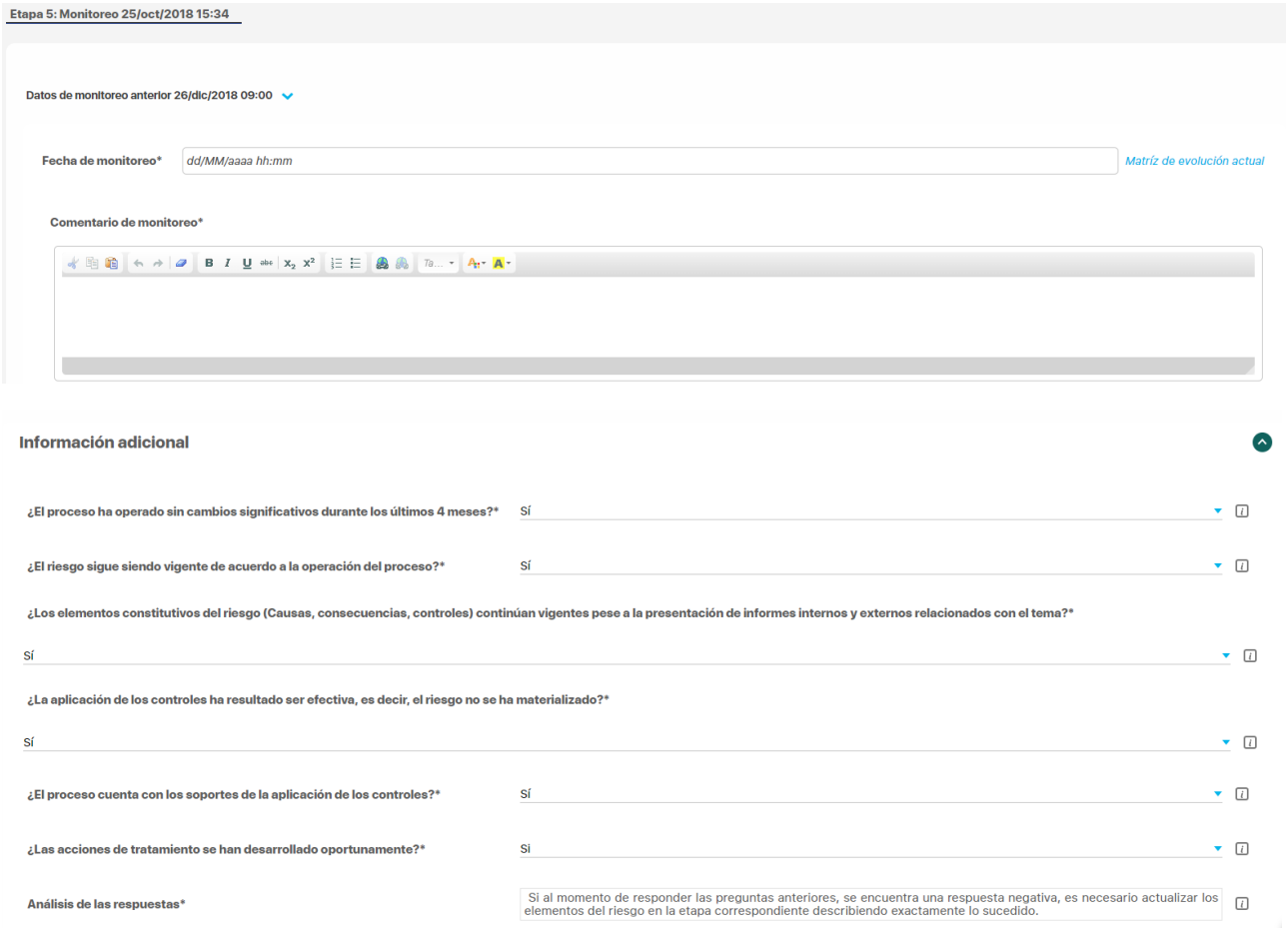


La tabla de la imagen anterior, contiene un resumen de los datos principales del riesgo, como el nombre, responsable, estado del riesgo, fecha de próxima revisión, materializaciones del riesgo y cumplimiento de fechas de monitoreo entre otras.

3. Monitorear el Riesgo

- De clic sobre el nombre del riesgo.
- Identifique la sección “Etapa 5: Monitoreo” y despliéguela de ser necesario a través de la flecha que así lo indica.
- En la pantalla que se despliega se deberán llenar los siguientes datos:
  a) Fecha de Monitoreo *(Campo obligatorio)*
  b) Información Adicional. *(Campo obligatorio)*
  En la sección “Información Adicional” se desplegarán 6 preguntas, las cuales deberán ser respondidas con “Sí” o “No” dependiendo de cada caso y tendrán un vínculo directo con lo descrito en el comentario de monitoreo.
  c) Comentario de Monitoreo *(Campo obligatorio)*
  Para el Comentario del Monitoreo se sugiere la siguiente redacción: *“Se realizó el Monitoreo del Riesgo, para lo cual se respondieron a todas las preguntas de manera afirmativa” o “Se realizó el Monitoreo del Riesgo, para lo cual, las preguntas (Indicar cuales) se respondieron de manera negativa y se hace necesario volver a analizar el riesgo” Para las preguntas ver punto b).*
  d) Fecha de Próximo monitoreo. *(Campo obligatorio)*
  Las fechas máximas de monitoreo establecidas por CISA son: 30 de abril, 30 de agosto y 31 de diciembre de cada Vigencia.
  e) Dar clic en “Programar otro monitoreo”

Nota: Si todas las preguntas del punto b) se responden de manera afirmativa el Monitoreo del Riesgo se registrará en el sistema hasta la siguiente fecha programada. Si por el contrario, alguna de las preguntas es respondida de manera negativa, se debe revisar la etapa del riesgo que se verá afectada y devolverla según corresponda de acuerdo a lo establecido en el punto “MONITOREO Y EVALUACIÓN”


Etapa 5: Monitoreo 25/oct/2018 15:34
Datos de monitoreo anterior 26/dic/2018 09:00
Fecha de monitoreo*
dd/MM/aaaa hh:mm
Matríz de evolución actual
Comentario de monitoreo*
Información adicional
¿El proceso ha operado sin cambios significativos durante los últimos 4 meses?*
Sí
¿El riesgo sigue siendo vigente de acuerdo a la operación del proceso?*
Sí
¿Los elementos constitutivos del riesgo (Causas, consecuencias, controles) continúan vigentes pese a la presentación de informes internos y externos relacionados con el tema?*
Sí
¿La aplicación de los controles ha resultado ser efectiva, es decir, el riesgo no se ha materializado?*
Sí
¿El proceso cuenta con los soportes de la aplicación de los controles?*
Sí
¿Las acciones de tratamiento se han desarrollado oportunamente?*
Si
Análisis de las respuestas*
Si al momento de responder las preguntas anteriores, se encuentra una respuesta negativa, es necesario actualizar los elementos del riesgo en la etapa correspondiente describiendo exactamente lo sucedido.

12. ANEXOS

ANEXO No. 1	Ficha técnica para el levantamiento de riesgos
ANEXO No. 2	Instructivo para la Gestión de Riesgos para Activos de Información

13. CONTROL DE CAMBIOS

Versión	Fecha	Motivo de la Revisión	Modificaciones
02	Diciembre 3 de 2008	Implementación del SIG en CISA.	Se ajustó a la nueva estructura documental y a la actual metodología sugerida por el DAFP.
03	Marzo 25 de 2009	Cambio de la estructura de la compañía	Se crearon las Vicepresidencias Comercial y Operación de Activos, se cambió el nombre a la Vicepresidencia de Operaciones a Vicepresidencia Administrativa y Financiera y en la Vicepresidencia Jurídica se concentraron los temas jurídicos del negocio, por lo tanto se asignaron los procesos correspondientes a cada Vicepresidencia.
04	Febrero 12 de 2010	Actualización de la metodología	Se adoptó la nueva metodología definida por el Departamento Administrativo de la Función Pública DAFP para la administración de riesgos, se incluyeron algunas definiciones y nuevas responsabilidades. Se incluye la herramienta de administración y control del SIG, para mantener la información relacionada.

Versión	Fecha	Motivo de la Revisión	Modificaciones
05	Septiembre 2 de 2011	Mejora del proceso	Se modificó el numeral 1 "Objetivo" Se modificó el numeral 2 "Responsables" Se modificó el numeral 3 "Términos y Definiciones" Se incluyó en el numeral 4 "Normatividad Legal y Aplicable", el requisito "NTC GP 1000:2009, numeral 4.1 "Requisitos Generales"" Se modificó el numeral 5.1 "Difusión y Socialización de los mapas y planes de tratamiento del riesgo" el cual se llama ahora "Difusión y socialización del mapa de riesgo". Se eliminó el numeral 5.3 "Manejo de Riesgos (Numeral 10.1.5 "Código de Buen Gobierno"). Igualmente se modificó la numeración de los numerales seguidos a este numeral. Se modificaron los numerales 5.3.1 "Procedimiento General", 5.3.2 "Estructura del proceso de Administración del Riesgo", 5.3.2.1 "Establecer el contexto estratégico", 5.3.2.1 "Análisis del Riesgo", 5.3.2.4 "Valoración del Riesgo", 5.3.2.5 "Políticas de Administración del Riesgo", 5.3.2.6 "Mapa de Riesgo", 5.3.2.7 "Monitoreo del Riesgo y Tratamiento del Riesgo Residual" Se modificó el numeral 6.1 "Procedimiento para la Administración del Riesgo en CISA"
06	Mayo 11 de 2012	Implementación NTC ISO 31000:2009	Se modificó todos los numerales de la Circular Normativa por la implementación de la metodología para la Gestión del Riesgo sugerida por la norma NTC ISO 31000:2009. Se eliminó el anexo No. 1 "Guía para la Administración del DAFP" Se crearon los anexos No. 1 "Evaluación de la eficacia del Control", No. 2 "Evaluación de la eficiencia del Control", No. 3 "Matriz de Probabilidad de Ocurrencia", No. 4 "Matriz de consecuencias, positivas o negativas" y No. 5 "Matriz Nivel del Riesgo".
07	Febrero 28 de 2013	Articulación metodología conforme Decreto 2641 de 2012, Artículo 1	Se modificaron los numerales 3 "Términos y Definiciones", 4 "Normatividad Legal y Aplicable", 5.3.2.3 "Identificación del Riesgo", 5.3.2.5 "Evaluación del Riesgo", 5.3.2.6

Versión	Fecha	Motivo de la Revisión	Modificaciones
			"Tratamiento del Riesgo" y 6.1 "Procedimiento para la Gestión del Riesgo en CISA".
08	Abril 29 de 2013	Cambio de Estructura de la Entidad	Se cambió en todo el cuerpo de la circular el nombre de la Gerencia de Planeación y Valoración por Gerencia de Planeación
08	Enero 17 de 2014	Inclusión Anexo	Se incluyó el anexo No. 6 "Instructivo para la Gestión de Riesgos para Activos de Información"
09	Febrero 9 de 2015	Mejora del Proceso	Se modificaron los numerales 2. "Responsables", 5.3.1 "Procedimiento General", 5.3.2.1 "Diseño del marco de referencia para la Gestión del Riesgo", 5.3.2.3 "Identificación del Riesgo", 5.3.2.4 "Análisis del Riesgo", 5.3.2.5 "Evaluación del Riesgo", 5.3.2.6 "Tratamiento del Riesgo" y 6.1 "Procedimiento para la Gestión del Riesgo en CISA".
09	Marzo 16 del 2015	Modificación Anexo	Se modificó el Anexo No. 6 "Instructivo para la Gestión de Riesgos para Activos de Información"
10	Agosto 14 del 2015	Mejora del Proceso	Se modificaron los numerales 2 "Responsables", 5.1 "Difusión y Socialización del Mapa de Riesgo",5.3.1 "Procedimiento General", 5.3.2.1 "Diseño del Marco de referencia para la Gestión del Riesgo" y 6.1 "Procedimiento para la Gestión del Riesgo en CISA"
11	Septiembre 25 de 2015	Actualización responsabilidades del procedimiento	Se modificó la actividad No. 13 "Presentar Mapa de Riesgos al Comité Asesor de Junta Directiva de Auditoria", del numeral 6.1 "Procedimiento para la Gestión del Riesgo en CISA".
12	Noviembre 18 de 2015	Mejora del Proceso	Se modificó el numeral 2 "Responsables", incluyendo la siguiente responsabilidad a los líderes de proceso: "De reportar a la Gerencia de Planeación, la materialización de los riesgos (Corrupción u operativos) inmediatamente se presente el evento."

Versión	Fecha	Motivo de la Revisión	Modificaciones
			Se modificó el anexo "Evaluación de la eficiencia del Control".
13	Junio 17 de 2016	Mejora de la metodología de riesgos	Se modificaron los numerales 1 "Objetivo", 1.1 "Objetivos específicos", 2 "Responsables", 3 "Términos y Definiciones", 4 "Normatividad Legal Aplicable", 5 "Políticas de Operación", el cual se llama ahora "Políticas de administración del riesgo", 5.4.2 "Identificación del riesgo", 5.5.1 "Análisis del riesgo", 5.5.4 "Evaluación del riesgo", el cual se llama ahora "Valoración del Riesgo", 5.6 "Tratamiento del riesgo" y 6.1 "Procedimiento para la gestión del riesgo de CISA". Se incluyeron los numerales 5.2 "Estrategia para la administración del riesgo", 5.3 "Lineamientos para el tratamiento de los riesgos", 5.4 "Identificación del riesgo", 5.4.1 "Establecimiento del contexto", 5.5.2 "Análisis de riesgos operativos", 5.5.3 "Análisis de riesgos de corrupción", 5.5.1 "Valoración de riesgos operativos", 5.5.5 "Valoración de riesgos de corrupción" y 5.7 "Difusión y socialización del mapa de riesgo" Se eliminaron los numerales 5.1 "Difusión y socialización del mapa de riesgo", 5.2 "Desarrollo del criterio para la evaluación del riesgo, 5.3 "metodología", 5.3.1 "Procedimiento General", 5.3.2 "Estructura para la gestión del riesgo" y 5.3.2.1 "Diseño del marco de referencia para la gestión del riesgo". Se eliminaron los anexos No. 1 "Evaluación de la eficacia del Control", No. 2 "Evaluación de la eficiencia del Control", No. 3 "Matriz de Probabilidad de Ocurrencia", No. 4 "Matriz de consecuencias, positivas o negativas" y No. 5 "Matriz Nivel del Riesgo". Se incluyeron los anexos 1 "Formato de levantamiento de Riesgos Operativos" y No. 2

Versión	Fecha	Motivo de la Revisión	Modificaciones
			"Formato de levantamiento de Riesgos de Corrupción". Se modificó el anexo No. 3 "Instructivo para la Gestión de Riesgos para Activos de Información".
13	Diciembre 14 de 2016	Actualización Anexo	Se modificó el anexo No. 3 "Instructivo para la Gestión de Riesgos para Activos de Información"
14	Septiembre 22 de 2017	Mejora del proceso	Se modificaron los numerales 2 "Responsables", 5.2.6.4 "Nivel de aceptación del riesgo de corrupción", 5.5.3 "Identificación, análisis y efecto de los controles existentes para el riesgo identificado", el cual ahora es el 5.2.6.5 "Identificación, análisis y efecto de los controles existentes para el riesgo de corrupción identificado, 5.2.8 "Tratamiento del riesgo". El numeral 5 "Políticas de administración del riesgo" se llama ahora "Políticas generales". Se incluyeron los numerales 5.1 "Generalidades", 5.2 "Política de administración de riesgos de CISA", 5.2.1 "Objetivo", 5.2.2 "Alcance", 5.2.6 "Valoración del riesgo de corrupción", 5.2.6.3 "Niveles para calificar el riesgo de corrupción", 5.2.7.1 "Niveles para calificar el riesgo operativo", 5.2.7.2 "Nivel de aceptación del riesgo operativo", 5.2.9 "Periodicidad para el seguimiento de acuerdo al nivel de riesgo residual", 5.2.10 "Niveles de responsabilidad sobre el seguimiento y evaluación de riesgos". Se eliminaron los numerales 5.2 "Estrategia para la administración del riesgo", 5.3 "Lineamientos para el tratamiento de los

Versión	Fecha	Motivo de la Revisión	Modificaciones
			riesgos", 5.4 "Identificación del riesgo", 5.5.5 "Valoración de riesgos de corrupción".
15	Mayo 25 de 2018	Actualización del documento conforme aprobación Comité Institucional de Coordinación de Control Interno del 17 de Mayo de 2018	Se actualizó la Política de administración del riesgo de CISA, de acuerdo con los lineamientos establecidos en el Modelo Integrado de Planeación y Gestión y en la Guía para la Administración del Riesgo versión 03 emitida por el Departamento Administrativo de la Función Pública (DAFP). Se cambió la denominación de la Circular Normativa de "Administración del Riesgo en Central de Inversiones S.A." por "Política de administración del riesgo en Central de Inversiones S.A." Se eliminaron los anexos "Formato de levantamiento de Riesgos Operativos" y "Formato de levantamiento de Riesgos de Corrupción" Se creó el formato "Ficha técnica para el levantamiento de riesgos"
16	Julio 30 de 2019	Mejora del proceso	Se actualizó el documento, considerando los lineamientos establecidos en la Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas v4. Se modificaron los anexos No. 1 "Formato para el levantamiento de riesgos" y No. 2 "Instructivo para la Gestión de Riesgos para Activos de Información"