CONTENIDO

Revisó	Aprobó
GERENTE DE PLANEACIÓN ESTRATÉGICA	GERENTE DE PLANEACIÓN ESTRATÉGICA
02/09/2021	02/09/2021

1. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

Con base en el Modelo Integrado de Planeación y Gestión - MIPG y de acuerdo con los lineamientos de la Dimensión de Direccionamiento estratégico y Planeación y en la Política de planeación Institucional, se dan las directrices para establecer una política alineada con los objetivos estratégicos que establezca la metodología para tratar y manejar los riesgos basados en su valoración, permitiendo tomar decisiones adecuadas y fijar lineamientos que serán transmitidos por la alta Dirección.

Para CISA la administración del riesgo es fundamental para lograr sus objetivos institucionales en el marco de su compromiso con la gestión transparente y los valores institucionales. La entidad reconoce que, en el desarrollo de sus actividades, se generan riesgos inherentes a la gestión de los diferentes procesos; por esta razón, CISA se compromete a definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten y que puedan afectar el logro de los objetivos, mediante la adopción de los mecanismos y acciones necesarias para darles el tratamiento adecuado, identificando, analizando, valorando y evaluando estos riesgos. Esta política de Administración del Riesgo contiene los lineamientos establecidos por la alta dirección y fue aprobada por el Comité de coordinación de control interno.

Con este documento se da cumplimiento a lo establecido en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, emitida por el Departamento Administrativo de la Función Pública, que contempla la metodología de administración del riesgo de gestión, corrupción y seguridad de la información y establece, la elaboración e implementación de la Política de Administración de riesgos.

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; así como, posibilitar la mejora continua en el proceso de toma de decisiones, teniendo en cuenta los siguientes aspectos:

- Fomentar la cultura de la prevención del riesgo en todos los niveles de la Institución.
- Mantener los controles que permitan el adecuado aprovechamiento de los recursos destinados a la ejecución de los procesos siempre bajo las mejores condiciones de eficacia, eficiencia, y efectividad.
- Gestionar de forma anticipada las vulnerabilidades o eventos que puedan afectar el logro de los objetivos institucionales.

3. ALCANCE

Esta Política contempla los riesgos estratégicos, operativos, corrupción, seguridad digital (ver Anexo “Instructivo para la Gestión de Riesgos de Seguridad Digital”) y continuidad del negocio, relacionados con todos los procesos que ejecuta CISA en cada una de las zonas.

No contempla los riesgos asociados a Sistema de Seguridad en el Trabajo, Gestión Ambiental, Lavado de Activos y Financiación del Terrorismo y Gestión de Proyectos toda vez que se tratan en normativas diferentes.

4. RESPONSABLES

Con el fin de asegurar que las responsabilidades y autoridades para la gestión del riesgo se asignan y comunican a los roles pertinentes, CISA determina las siguientes responsabilidades de acuerdo con las líneas de Defensa definidas en la Guía para la administración de los riesgos y diseño de controles del Departamento Administrativo de la Función Pública - DAFP:

LÍNEA ESTRATÉGICA - ALTA DIRECCIÓN:

- Revisar y analizar las propuestas presentadas por la Gerencia de Planeación Estratégica, de la Política de Administración del Riesgo y formalizarlas, para la implementación en CISA.
- Promover la administración de riesgos como un componente fundamental dentro de la operación de CISA.
- Realizar seguimiento periódico al cumplimiento de la Política de Administración de Riesgos definiendo acciones de mejora ante posibles desviaciones.
- Aprobar el marco de apetito de riesgo para CISA y asegurarse que es coherente con los objetivos estratégicos, el modelo de negocio y la capacidad de riesgo.
- Supervisar el marco de apetito de riesgo con el objetivo de asegurar que se tomen las medidas adecuadas con respecto a niveles no aceptables o de potenciales incumplimientos en los límites de apetito, tolerancia y capacidad de riesgo.
- Ser responsable de la integridad del marco de apetito de riesgo, incluyendo la identificación oportuna y los protocolos de escalamiento de toma de decisión cuando se deban aumentar los límites de riesgo y de exposiciones materiales.
- Evaluar el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento del este.
- Aprobar los riesgos relacionados con la interrupción de continuidad del negocio.

PRIMERA LÍNEA DE DEFENSA - LÍDERES DE PROCESO Y EQUIPO OPERATIVO: Responsables de gestionar los riesgos y hacer seguimiento en 1ª línea.

- Establecer y revisar el contexto institucional (interno y externo), así como de definir las partes interesadas para su proceso.
- Asegurar que la construcción de los riesgos asociados al proceso se realice de forma participativa.
- Identificar, analizar, evaluar y valorar los riesgos del proceso a través del anexo “Ficha Técnica para el levantamiento de Riesgos (Matriz de Riesgos)” (aplica para los riesgos nuevos).
- Actualizar la matriz de riesgos por lo menos una vez al año (mes noviembre) a través del anexo “Matriz de Riesgos” y enviar a la Gerencia de Planeación Estratégica la misma actualizada; con el fin de identificar los cambios en la evolución de los controles y perfil de riesgo
- Realizar el monitoreo a los riesgos del proceso a través del Aplicativo de Seguimiento a la Estrategia (ASE).
- Divulgar a todos los colaboradores a cargo, el mapa de riesgos operativo y de corrupción de proceso incluyendo las zonas.
- Asegurar la ejecución de los controles, su correcta documentación, aplicación, fortalecimiento e implementación de acciones de tratamiento sobre el riesgo.

- Realizar seguimiento periódico al comportamiento de los riesgos y en caso de su eventual materialización seguir lo mencionado en el ítem “Materialización del Riesgo” en adelante y reportar a la Gerencia de Planeación Estratégica.
- El equipo operativo debe servir de enlace directo entre el proceso y la Gerencia de Planeación Estratégica para garantizar la aplicación de las metodologías aquí desarrolladas.
  Cooperar con la Gerencia de Planeación Estratégica cuando se requiera evaluar cómo el marco de apetito de riesgo ha sido incorporado en la gestión de sus procesos.

SEGUNDA LÍNEA DE DEFENSA - GERENCIA DE PLANEACIÓN ESTRATÉGICA: Capacita, acompaña, genera recomendaciones, define metodología.

- Generar propuestas sobre la metodología y Políticas para la Administración del Riesgo de la Entidad y presentarlas para aprobación del Comité Institucional de Coordinación de Control Interno.
- Coordinar, liderar, capacitar y asesorar a la primera línea de defensa en la aplicación de la metodología y políticas desarrolladas.
- Realizar un monitoreo independiente al cumplimiento de las etapas para la administración del riesgo.
- Consolidar el mapa de riesgos institucionales y socializarlo con las partes interesadas.
- Cargar en el Aplicativo de Seguimiento a la Estrategia (ASE) los riesgos identificados y previamente aprobados.
- Reportar lo que corresponda por incumplimientos a la Gerencia de Recursos.
- Establecer un marco de apetito de riesgo adecuado para CISA, consistente con los objetivos estratégicos y el modelo de negocio.
- Obtener la aprobación del Comité Institucional de Gestión y Desempeño sobre el marco de apetito de riesgo e informar al menos una vez por semestre sobre el perfil de riesgo de CISA.
- Ser responsable de la integridad del marco de apetito de riesgo, incluyendo la identificación oportuna y los protocolos de escalamiento de toma de decisión cuando se deban aumentar los límites de riesgo y de exposiciones materiales.
- Realizar un seguimiento semestral de las actividades con aceptación y exposiciones al riesgo en consonancia con el apetito al riesgo, la capacidad de riesgo y el correspondiente marco definido por el Comité Institucional de Gestión y Desempeño.
  Presentar trimestralmente al Comité asesor de Junta Directiva de Auditoría un reporte ejecutivo con el resultado del seguimiento de la política de riesgos no financieros.

Analista de procesos y continuidad del negocio:

- Asesorar a los líderes de los procesos críticos frente la gestión de riesgos de continuidad del negocio.

Oficial de Seguridad de la información:

- Definir el procedimiento para la Identificación y Valoración de Activos.
- Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento).
- Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos.
- Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.

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.
- Evaluar la efectividad y la aplicación de controles; así como también las actividades de monitoreo vinculadas a riesgos de CISA.
- Verificar que los controles están diseñados e implementados de manera efectiva y operen de forma efectiva para mitigar los riesgos.
- Reportar sobre la posibilidad de riesgo de fraude o corrupción en los procesos auditados de acuerdo con lo dispuesto en el Memorando Circular No. 046 "Política para la Prevención de Corrupción y Procedimiento para la Gestión de Reportes de Actos de Corrupción".
- Realizar seguimiento a las acciones establecidas en los planes de tratamiento en los procesos auditados.
- Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos.
- Proporcionar aseguramiento objetivo en los procesos identificados no cubiertas por la segunda línea de defensa.
- Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados al Comité de Coordinación de Control Interno.
- Recomendar mejoras a la política de administración del riesgo.

5. INSTITUCIONALIDAD

El modelo integrado de planeación y gestión (MIPG) define para su operación articulada la creación en todas las entidades el Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017 y el Comité Institucional de Coordinación de Control Interno, reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017, en este marco general, para una adecuada gestión del riesgo, dicha institucionalidad entra a funcionar de la siguiente forma:

- **Comité Institucional de Gestión y Desempeño:** Analiza la gestión del riesgo y se aplican las mejoras que considere pertinentes.
- **Comité Institucional de Coordinación de Control Interno:** Se traslada el análisis de eventos y riesgos críticos.

6. TÉRMINOS Y DEFINICIONES [1]

Administración de riesgos	Conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.

1 Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades públicas, ISO 31000

Amenaza	Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización las cuales pueden ser factores no controlables por CISA.
Activo de la información	En el contexto de seguridad digital es todo activo que posee información para CISA. Ej.: la información física, y digital; el software; el hardware; los servicios de información, de comunicaciones, de almacenamiento, etc.; las personas y otros.
Análisis del riesgo	Etapa que establece la probabilidad de ocurrencia del riesgo e impacto, con el fin de estimar la zona de riesgo inherente.
Apetito del riesgo	Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
Calificación del riesgo	Estimación independiente de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
Causa	Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo; entendido paralelamente como evento de interrupción.
Causa inmediata	Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.
Causa raíz	Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
Confidencialidad	Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
Capacidad de riesgo	Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.
Consecuencia	Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la Entidad, sus grupos de valor y demás partes interesadas.
Control	Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).
Control correctivo	Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones); está orientado a disminuir el nivel de impacto del riesgo.
Control preventivo	Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones); está orientado a disminuir la probabilidad de ocurrencia del riesgo.
Corrupción	Abuso de posiciones de poder o de confianza, para el beneficio particular en detrimento del interés colectivo, realizado a través de ofrecer o solicitar, entregar o recibir bienes o dinero en especie, en servicios o beneficios, a cambio de acciones, decisiones u omisiones.

Debilidad	Situación interna que la Entidad puede controlar y que puede afectar su operación.
Disponibilidad	Propiedad de ser accesible y utilizable a demanda por una entidad.
Dueño del riesgo	Es el líder del proceso al cual corresponda el riesgo identificado.
Evaluación del riesgo	Etapa que establece el cruce cuantitativo de las calificaciones de probabilidad e impacto, antes y después de controles.
Evento	Presencia o cambio de un conjunto particular de circunstancias.
Factores de Riesgos	Se entiende por factores de riesgo, las fuentes generadoras de eventos en las que se originan las pérdidas por riesgo. Son factores de riesgo el recurso humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos. Elementos o escenarios que solos o en combinación pueden hacer uso de una debilidad para generar un perjuicio o impacto negativo en la organización (Materializar el riesgo), o los medios potenciales por los cuales las vulnerabilidades pueden ser explotadas u ocasionadas.
Formato levantamiento de riesgos	Herramienta de la Entidad, que contempla las orientaciones para ejecutar cada una de las etapas de administración del riesgo.
Gestion 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.
Herramienta de administración del SGSI-módulo riesgos	Software de administración del sistema de seguridad de la información.
Identificación del riesgo	Etapa proceso para encontrar, reconocer y describir el riesgo.
Impacto	Las consecuencias que puede ocasionar a la organización la materialización del riesgo.
Integridad	Propiedad de exactitud y completitud.
Líneas de defensa	Es un modelo de control que establece los roles y responsabilidades de todos los actores del riesgo y control en una Entidad, este proporciona aseguramiento de la gestión y previene la materialización de los riesgos en todos sus ámbitos.
Mapa de riesgos	Documento con la información resultante de la gestión del riesgo.
Materialización del riesgo	Ocurrencia de un riesgo identificado o no identificado de la Entidad.
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.
Nivel de riesgo	Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad *

	Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.
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.
Perfil de riesgo	Descripción de cualquier conjunto de riesgos
Política de Administración del Riesgo	Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.
Probabilidad	Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
Procedimiento	Es una forma específica para llevar a cabo una actividad o un proceso
Proceso	Un proceso es un conjunto de actividades que están interrelacionadas y que pueden interactuar entre sí. Estas actividades transforman los elementos de entrada en resultados, para ello es esencial la asignación de recursos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.
Riesgo	Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
Riesgo inherente	Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
Riesgo residual	El resultado de aplicar la efectividad de los controles al riesgo inherente.
Tratamiento del riesgo	Es el proceso para modificar el riesgo, el tratamiento del riesgo puede implicar evitar el riesgo decidiendo no iniciar o continuar la actividad que lo causó, incrementar el riesgo para conseguir una oportunidad, suprimir la fuente del riesgo, cambiar la probabilidad, cambiar las consecuencias o retener el riesgo mediante una decisión informada.
Tolerancia del riesgo	Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.
Valoración del Riesgo	Etapa que establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa se determina el riesgo residual, la opción de manejo a seguir y si es necesario, las acciones a desarrollar para el fortalecimiento de controles.
Vulnerabilidad	Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

7. 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.
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.
Ley 1712 de 2014	Ley de Transparencia y de Acceso a la Información Pública, reglamentada parcialmente por el Decreto Nacional 103 de 2015.
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.

8. 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* [2], *este efecto es una desviación de aquello que se espera sea positivo, negativo o ambos.* Según lo anterior, CISA enfrenta factores que influencian interna y externamente, creando incertidumbre sobre el cumplimiento de los objetivos de CISA, es este lo que se denomina riesgo.

En este sentido, *"la administración de riesgos es un método lógico y sistemático para establecer el contexto, identificar, analizar, valorar, 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"*.[3]

2 NTC ISO 31000:2009

3 Norma Australiana ASNZ4360 de 1999

Todos los procesos de CISA intrínsecamente poseen riesgos que pueden afectar el cumplimiento de los objetivos previstos; por lo tanto, es necesario tomar medidas, para identificar las posibles causas y consecuencias que podría conllevar la materialización de dichos riesgos.

9. MARCO CONCEPTUAL DEL APETITO DE RIESGO

Es la guía que da como base del marco de acción para la toma de decisiones por parte de la Alta Dirección, la cual influye en la forma de operar de CISA y en la cultura frente a la gestión de los riesgos. Este marco contempla un conjunto de lineamientos con los límites a partir de los cuales CISA establece, comunica y monitorea el nivel de apetito por el riesgo.
El objetivo del marco de apetito del riesgo es proporcionar un conjunto integrado de medidas que le permiten a CISA determinar los tipos de riesgos que desea asumir, tratar, mitigar, compartir o evitar, basados en la calificación residual del riesgo, determinada por su posición en el mapa de calor para la administración de riesgos.

9.1 Declaración del apetito del riesgo

CISA tiene como objetivo mantener su riesgo residual deseable la zona de riesgo residual “bajo” o “moderado”, el cual le permitirá, mitigar la incertidumbre y de este modo generar condiciones que le permitan alcanzar el logro de sus objetivos, sin embargo, para los riesgos de corrupción solo será admisible encontrase en el recuadro “moderado” con “rara vez”. Cualquier riesgo, que se encuentre dentro de las zonas antes mencionadas, no requerirán generar planes de tratamiento para fortalecer su administración, sino mantener los controles identificados y realizar el monitoreo permanente de los mismos.
Con respecto a la capacidad del riesgo, serán considerados los riesgos que se encuentren en la zona de riesgo residual “alto” o “extremo”, y para los riesgos de corrupción “moderado con imposible”, “moderado con posible”, esto implica que a diferencia con lo anterior, que se deberán ejecutar planes de tratamiento que permitan mitigar, compartir o eliminar el riesgo, basados en la ejecución de actividades que permitan el fortalecimiento o generación de nuevos controles para contrarrestar los impactos que pueden suceder tras la materialización de un evento.

9.2 Comunicación marco integral de apetito de riesgo

El marco de apetito de riesgo debe ser adecuadamente comunicado en todos los niveles de CISA. Esto con el fin de que sea considerado en el marco de la toma de decisiones; los grupos de interés que se debe comunicar dicho marco son: Junta directiva, Alta dirección y líderes de los procesos.

10. ESTABLECIMIENTO DEL 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 del proceso y de la Entidad. Definir el contexto institucional contribuye al autoconocimiento de la Entidad frente a la exposición al riesgo, ya que permite identificar las situaciones generadoras de riesgos.

El establecimiento del contexto permite a CISA articular los objetivos frente a las características del entorno interno y externo en el cual opera, los cuales deberán ser considerados posteriormente en la gestión del riesgo.

El contexto de CISA se determinó por medio de la metodología DOFA, la cual permite identificar los aspectos clave a considerar para definir el alcancé de los objetivos y potencializar las fortalezas y oportunidades, así como también minimizar el riesgo asociado a las debilidades y amenazas; para lo cual se evaluó con el líder de cada proceso las fortalezas y debilidades en relación con las oportunidades y amenazas que ellos identifican en la operación.

Algunos de los componentes evaluados fueron:

Tipo de contexto	Definición	Ejemplos
Establecimiento del contexto del proceso	Se determinan las características o aspectos esenciales del proceso y sus interrelaciones.	Objetivo, alcance, interrelaciones existentes, procedimientos y responsables del proceso.
Establecimiento del contexto interno	Se determinan las características o aspectos esenciales del entorno en el cual opera la entidad.	Estructura organizacional, funciones y responsabilidades, políticas, objetivos y estrategias, recursos y conocimiento y cultura organizacional.
Establecimiento del contexto externo	Se determinan las características o aspectos esenciales del ambiente en el cual la organización busca alcanzar sus objetivos.	Político, económico y financiero, social y cultural, tecnológico, ambiental y legal.

El contexto institucional de CISA se revisará teniendo en cuenta los cambios administrativos que puedan afectar la operación, está se realizará por lo menos cada dos años mediante un ejercicio ejecutado por los líderes de proceso quienes garantizaran la participación de sus equipos de trabajo junto con el apoyo y direccionamiento de la Gerencia de Planeación Estratégica.

Nota. Cada vez que se identifique una causa del riesgo esta deberá relacionarse con un factor de riesgo interno.

10.1 Establecimiento del contexto a nivel de procesos

Se define que todos los procesos deberán estar debidamente documentados y actualizados; así las cosas, los siguientes son elementos mínimos que se deberán considerar y documentar en el establecimiento del contexto en cada uno de los procesos del mapa de procesos de CISA:

Factores de Riesgo del Proceso	Descripción
Diseño del proceso	Claridad en la descripción del alcance (misión y visión). Objetivos estratégicos vinculados al proceso.

Factores de Riesgo del Proceso	Descripción
	Objetivo del procesos y características claves. Actividades clave utilizadas por el proceso para el cumplimiento del objetivo. Sistemas de información utilizados en la operación.
Interacciones con otros procesos	Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes. Proveedores o terceros que soportan el proceso. Cantidad de ciudadanos afectados por el proceso.
Procedimientos asociados	Pertinencia en los procedimientos que desarrollan los procesos. Caracterización del proceso.
Responsable del proceso	Grado de autoridad y responsabilidad de los funcionarios frente al proceso. Estructura organizacional que soporta el proceso.
Comunicación entre los procesos	Efectividad en los flujos de información determinados en la interacción de los procesos, así como la toma de decisiones.

10.2 Establecimiento del contexto interno

El contexto interno es el ambiente interno en el cual CISA busca alcanzar sus objetivos. Es importante que la administración del riesgo este alineada con la cultura, los procesos, la estructura y la estrategia de la organización. Para este análisis se tuvieron en cuenta los factores internos como las debilidades y fortalezas más relevantes (número de veces mencionada por el área), el resultado es el siguiente:

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

Factores de Riesgo	Clasificación del riesgo DAFP	Clasificación del riesgo CISA	Situaciones
Talento Humano: Se analiza posible dolo e intención frente a la corrupción.	**Fraude interno:** Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abusos de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son	**Comportamiento humano**	Existe cierto riesgo de que la Entidad sufra pérdidas causadas por hurto de activos, compromiso y comportamiento no ético (principios y valores) de los empleados, fraude interno, corrupción y/o soborno.

Factores de Riesgo	Clasificación del riesgo DAFP	Clasificación del riesgo CISA	Situaciones
	realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros		
	Relaciones laborales: Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación	**Ambiente laboral**	Existe cierto riesgo de que la entidad sufra pérdidas causadas por ambiente laboral desfavorable.
	Usuarios, productos y prácticas: Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.	**Actividades Individuales**	Existe cierto riesgo de que la entidad sufra pérdidas causadas por negligencia, error humano, personal no cuenta con las aptitudes y destrezas necesarias para afrontar la exigencia de los procesos, inadecuada contratación, estabilidad laboral y disponibilidad de personal.
Tecnología: Eventos relacionados con la infraestructura tecnológica de la entidad.	**Fallas tecnológicas:** Errores en hardware, software, telecomunicaciones y/o interrupción de servicios básicos.	**Aspectos tecnológicos**	Existe cierto riesgo de que la Entidad sufra pérdidas causadas por uso inadecuado de los sistemas de información, comunicación y/o tecnologías inherentes en los procesos, hechos que atenten contra la confidencialidad, integridad, operación, disponibilidad, vigencia, pertinencia, estado de los sistemas de información, daño a equipos, caída de los aplicativos o redes, errores en los programas, fallas en la parametrización, bases de datos reducidas, falta de automatización de procesos y/o automatizar nuevas líneas de negocio.
Procesos: Eventos relacionados con errores en las	**Ejecución y administración de procesos**: Pérdidas	**Procesos internos**	Existe cierto riesgo de que la Entidad sufra pérdidas causadas por diseño inadecuado de los

Factores de Riesgo	Clasificación del riesgo DAFP	Clasificación del riesgo CISA	Situaciones
actividades que deben realizar los servidores de la organización.	derivadas de errores en la ejecución y administración de procesos.		procesos internos o que hayan fijadas unas políticas inadecuadas que mermen el desarrollo de las operaciones e impidan ofrecer un producto o servicio de calidad, políticas rígidas, falta de sinergia entre los procesos, procesos desagregados, falta de entendimiento de los objetivos estratégicos o del proceso, falta de capacitación, sistemas de información y/o falta de mejora continua.
		Actividades y Controles gerenciales	Existe cierto riesgo de que la Entidad sufra pérdidas causadas por los mecanismos de seguimiento y medición institucionales, errores en la grabación de los negocios o autorizaciones, falta de información para la toma de decisiones, gestión deficiente de proveedores y contingencias legales.
		Aspectos técnicos	Existe cierto riesgo de que la Entidad sufra pérdidas causadas por fallas en la capacidad operativa en la respuesta del desarrollo de sus funciones y/o obligaciones (inoportunidad en la entrega de productos/servicios), insuficiencia de inventario de inmuebles, falta de información en el mercado de inmuebles, modelos de valoración no ajustado a las necesidades actuales, estructura de costos alta, procesos de contratación mixta, falta de planificación a corto plazo, nuevas líneas de negocio y variedad de activos por vender.

Como base en esta información se definen y priorizan las oportunidades de mejora, fortalezas de la entidad frente a su contexto interno; y a su vez, se enfocan los esfuerzos en las debilidades con acciones que permitan la mitigación a la exposición de potenciales riesgos.

10.3 Establecimiento del contexto externo

El contexto externo es el ambiente externo en el cual CISA busca alcanzar sus objetivos. Entenderlo es importante para garantizar que los objetivos y las precauciones de las partes interesadas externas se tomen en consideración en el momento de tomar decisiones.

Para el análisis de contexto externo, se tuvieron en cuenta los factores externos como las oportunidades y amenazas más relevantes (número de veces mencionada por el área), el resultado es el siguiente:

Factores de Riesgo	Clasificación del riesgo DAFP	Clasificación del riesgo CISA	Situaciones
Infraestructura: Eventos relacionados con la infraestructura física de la entidad.	**Daños a activos fijos/ eventos externos:** Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.	**Eventos naturales**	Existe cierto riesgo de que la Entidad sufra pérdidas causadas por emisiones, residuos generados y dispuestos de forma errónea, cortes de energía, catástrofes naturales, incendios, fallas en el desarrollo sostenible del ambiente, fallas en los servicios públicos o pandemias.
Eventos externos: Situaciones externas que afectan la entidad.	**Fraude externo:** Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).	**Fraude externo**	Existe cierto riesgo de que la Entidad sufra pérdidas causadas por actos delictivos, ataques cibernéticos, robos, atentados o vandalismo.
	Otros eventos externos: Pérdida derivada de	**Circunstancias políticas**	Existe cierto riesgo de que la Entidad sufra pérdidas causadas por cambios de gobierno, legislación, planes, políticas públicas, decisiones gubernamentales, nuevas líneas de negocio,

Factores de Riesgo	Clasificación del riesgo DAFP	Clasificación del riesgo CISA	Situaciones
	otros eventos externos diferentes a los relacionados con fraude externo o infraestructura.		participación directa con el gobierno o cobro de comisiones fijas para la venta de inmuebles.
		Económicas (por la falta de recursos)	Existe cierto riesgo de que la Entidad sufra pérdidas causadas por capacidad financiera de la entidad o administración de los recursos disponibles.
		Relaciones comerciales y legales	Existe cierto riesgo de que la Entidad sufra pérdidas causadas por bajo reconocimiento o posicionamiento en el mercado, uso inadecuado de redes sociales, estrategias de marketing ineficientes, clientes con posibles dependencias, relacionamientos inadecuados con clientes externos y contratación ineficientes.
		Entorno digital	Clientes, proveedores de servicios y empresas que sean competencia directa y/o se relacionen con la misión de la entidad. Normativas o aspectos jurídicos que apliquen directa o indirectamente a la entidad. Dependencias económicas y financieras por parte de otras empresas. Entorno Cultural Cualquier otro factor externo de tipo internacional, nacional (gobierno), regional o local. Cantidad de ciudadanos a los cuales la entidad pública brinda servicios a través del entorno digital como trámites a través de páginas web. Aspectos externos que pueden verse afectados con los riesgos de seguridad digital, tales como el ambiente social, económico y ambiental que tengan alguna relación con las operaciones asociadas a la entidad.

Este listado de amenazas y oportunidades del entorno son consideradas parte de la identificación de riesgos y en el establecimiento de los objetivos que permitan potencializar esas oportunidades.

11. ESTRUCTURA 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 de la gestión del riesgo; en la descripción se explicarán los aspectos conceptuales y operativos que se deben tener en cuenta.
Las etapas de identificación, análisis, valoración y tratamiento se realizarán utilizando como herramienta el anexo “Ficha Técnica para el levantamiento de Riesgos (Matriz de Riesgos)” y la etapa de monitoreo / revisión

se realizará a través del Aplicativo de Seguimiento a la Estrategia (ASE), descrito en el anexo "Instructivo para el monitoreo de riesgos en el aplicativo de seguimiento a la estrategia – ASE".

11.1 IDENTIFICAR EL RIESGO

Es el proceso para encontrar, reconocer y describir el riesgo, cuyo ejercicio debe ser participativo, que por lo general se lleva a cabo entre el líder del proceso y su equipo colaborador con el apoyo de la Gerencia de Planeación Estratégica, con el fin de realizar un análisis de las actividades ejecutadas por el proceso e identificar los posibles riesgos asociados.

El riesgo está directamente relacionado con los atributos de calidad previamente definidos en los productos, los cuales son generados en los procesos, dado lo anterior, 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.

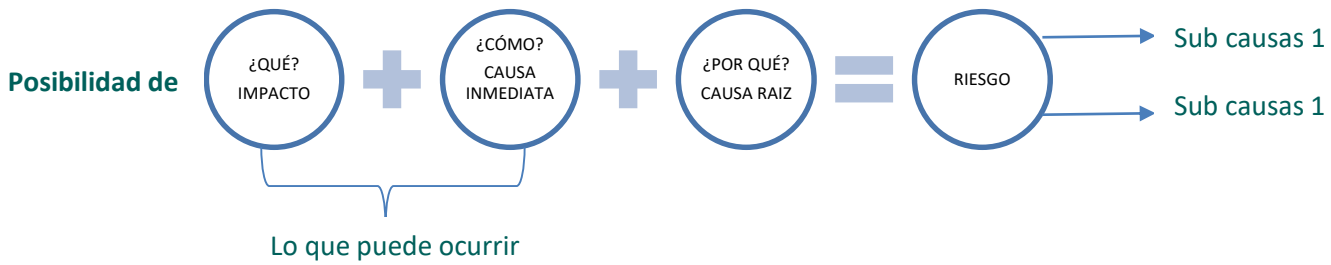
En este orden de ideas, para identificar un riesgo, es necesario realizar los siguientes pasos:

Paso		Descripción	Fuente de Información
1	**Revisión del objetivo y alcance del proceso.**	1. Seleccionar un proceso y determinar qué hace, para qué lo hace y cómo lo hace. 2. Evaluar que los objetivos del proceso cumplan con las características SMART: Especifico, Medible, Alcanzable, Relevante (relacionado con un objetivo estratégico), 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 pude impactar directamente sobre el alcance y los productos que de este se generan. La Jefatura de procesos y productividad deberá ser garante de mantener actualizada esta información. 3. Revisar el alcance: dónde inicia y finaliza la gestión del proceso y qué actividades contempla. 4. Determinar cuáles son las salidas del proceso generadas durante la ejecución de este. 5. Si el riesgo es de tipo estratégico, se deberá evaluar el objetivo estratégico, en cumplimiento con las características SMART.	Caracterización del proceso

Paso		Descripción	Fuente de Información
		6. Identificar cuáles son las actividades dentro del flujo del proceso donde se evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo* y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.	
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 del producto a analizar: experiencias pasadas, riesgos materializados, problemas generados en la Entidad o en el proceso, informes y conceptos de expertos, informes de la Auditoría Interna y entes de control e 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, análisis de la información de evaluaciones previas del proceso, informes de gestión y demás, servirán como insumo principal para describir los riesgos que podrían suscitarse, dado el incumplimiento a las características del producto.	Descripción del riesgo

11.1.1 Describir el riesgo

La descripción del riesgo se deberá realizar con la siguiente estructura:



Desglosando la estructura, se tiene:

- Posibilidad seguido del impacto,
- **Impacto:** Es la consecuencia que puede ocasionar a la organización la materialización del riesgo.
- **Causa inmediata:** circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.
- **Causa raíz:** es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o sub causas que pueden ser analizadas.

Al momento de describir el riesgo, es importante no 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…".

Aspectos para tener en cuenta en la descripción identificación de los riesgos de corrupción:
Con el fin de facilitar la identificación y correcta clasificación, 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 clasifica como **Riesgo de Corrupción**.
A continuación, se presenta una variable respecto de la identificación de las causas para los riesgos de corrupción, frente a los riesgos operativos:

- Riesgos operativos nos preguntamos *¿por qué?* se puede presentar la situación descrita en el riesgo.
- Riesgos 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.

11.1.2 Clasificar el riesgo

Durante esta etapa se realiza la clasificación del riesgo según sus características, de este modo, en CISA clasificaremos los riesgos en:

Clases de riesgo	Definición
Estratégico	Está relacionado con el cumplimiento de los objetivos estratégicos, la definición de políticas, diseño y conceptualización de la entidad por parte de la Alta Dirección. En resumen, son aquellos riesgos que se asociarán directamente con la Estrategia de CISA.
Operativo	El riesgo operativo hace referencia a la posibilidad de que una entidad incurra en pérdidas originadas por fuentes como errores humanos, fallas tecnológicas o procesos, infraestructura, o por factores externos. Dentro de esta categoría se incluirán los riesgos financieros (relacionados con el manejo de los recursos de la entidad: ejecución presupuestal, elaboración estados

Clases de riesgo	Definición
	financieros, pagos, manejos de excedentes de tesorería y manejo de los bienes), legales y reputacionales.
Corrupción	Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
Seguridad Digital	Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias [4].
Continuidad del Negocio	Es la posibilidad de interrupción que pueda afectar la continuidad de las operaciones críticas de CISA, a través de la indisponibilidad de instalaciones, tecnología, personal, información y proveedores.

Nota: *Los lineamientos para la administración de riesgos de Seguridad Digital se especifican en el anexo "Instructivo para la Gestión de Riesgos de Seguridad Digital" de la presente Circular Normativa.*

11.1.3 Describir la posible materialización del riesgo

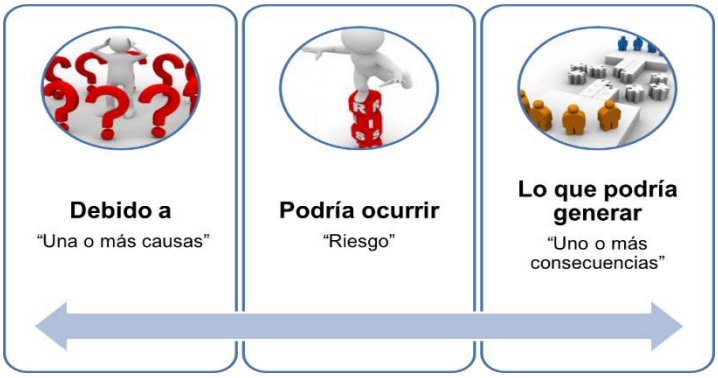
La identificación del riesgo no consiste únicamente en la identificación de sus causas y consecuencias, sino que también se hace necesario, establecer con claridad cuándo se entenderá materializado el riesgo permitiendo a cualquier empleado considerar con precisión los aspectos para tener en cuenta, en adelante se entenderá como la materialización objetiva del riesgo.

La identificación de la acción que materializará el riesgo debe estar en completa armonía con las causas identificadas y con el mismo riesgo, para lo cual se hace necesario realizar una descripción detallada del evento que posiblemente lo provocará, lo que, en su momento dará entrada a los análisis descritos en el numeral "Materialización de los Riesgos" de la presente circular normativa.

11.1.4 Concepto Integral del Riesgo

La identificación del riesgo no se puede realizar de manera fragmentada; debe existir una relación integral entre las causas, 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 debe establecer un método apropiado que consiste en el uso del metalenguaje del riesgo para una identificación estructurada en tres partes:

[4] ISO/IEC 27000



El esquema anterior pretende identificar correctamente las causas, riesgo y consecuencias, sin confundir unas con otras; de no ser así, los pasos posteriores quedan viciados de error.

11.1.5 Identificar los factores del riesgo y clasificación del riesgo

Son el resultado del análisis del contexto institucional, los cuales servirán de referencia para determinar las posibles causas generadoras de riesgo, por esta razón, cada una de estas deberá estar asociada a un factor de riesgo, según corresponda.

A continuación, una tabla que referencia los factores a usar:

Tipo de factor de riesgo	Factores de riesgo	Clasificación del riesgo DAFP	Clasificación del riesgo CISA
Interno	**Talento Humano**	Fraude interno	Comportamiento humano
		Relaciones laborales	Ambiente laboral
		Usuarios, productos y prácticas	Actividades Individuales
	Tecnología	Fallas tecnológicas	Aspectos tecnológicos
	Procesos	Ejecución y administración de proceso	Procesos internos
			Diseño del proceso
			Interacciones con otros procesos
			Procedimientos asociados
			Responsable del proceso
			Comunicación entre los procesos
			Actividades y Controles gerenciales
			Aspectos técnicos
Externo	**Infraestructura**	Daños a activos fijos/ eventos externos	Eventos naturales
	Eventos externos	Fraude externo	Fraude externo
		Otros eventos externos	Circunstancias políticas

Tipo de factor de riesgo	Factores de riesgo	Clasificación del riesgo DAFP	Clasificación del riesgo CISA
			Económicas (por la falta de recursos)
			Relaciones comerciales y legales
			Entorno Digital

11.1.6 Identificar causas del riesgo

Las causas son todos aquellos factores* internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo[5]. Se debe garantizar la identificación y coherencia entre las causas significativas y el riesgo identificado, teniendo en cuenta que los controles estarán orientados a la eliminación o mitigación de las 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"* [6].

11.1.7 Identificar las consecuencias del Riesgo

Son los efectos o situaciones resultantes de la materialización del riesgo que pudieran impactar en el proceso, la Entidad, grupos de valor y demás partes interesadas [7]; generalmente, son sobre bienes materiales o inmateriales con incidencias importantes tales como: daños físicos, fallecimiento, sanciones, pérdidas económicas, de información, de bienes, de imagen, credibilidad y confianza, interrupción del servicio o daño ambiental, entre otras que pudiesen ocasionarse. Se debe garantizar que cada consecuencia identificada este relacionada con el riesgo y los controles.

11.2 ANALIZAR EL RIESGO

Esta etapa busca establecer para cada riesgo, la probabilidad de ocurrencia e impacto[8] de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información cuantitativa y cualitativa para establecer el nivel de riesgo inherente.
La calificación del riesgo inherente se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede ocasionar su materialización.

5 Guía para la administración del riesgo y el diseño de controles en entidades públicas

6 Guía metodológica para la administración del riesgo IDPAC

7 Guía para la administración del riesgo y el diseño de controles en Entidades públicas

8 Se han establecido dos aspectos para tener en cuenta en el análisis de los riesgos identificados: probabilidad e impacto, la primera se entiende como la posibilidad de ocurrencia del riesgo y puede ser medida a partir de la frecuencia y la segunda se entiende la consecuencia que puede ocasionar a la Entidad en caso de materialización del riesgo.

11.2.1 Cálculo de la probabilidad inherente

Puntualmente para la calificación de la probabilidad, se deben tomar como base 2 escenarios:

11.2.1.1 Escenario 1: Riesgo totalmente nuevo

Con respecto a la probabilidad inherente del riesgo para aquel que es totalmente nuevo, es decir, que no se encontraba descrito dentro de la matriz de riesgos, ni el mismo, ni otro que lo fuese a remplazar, se calculará basados en la exposición que enfrenta el proceso respecto del riesgo que esté analizando, siendo determinado por el número de veces que se desarrolla la actividad expuesta al riesgo en el periodo de un año (los últimos doce meses). La selección para ese escenario se basará en la siguiente tabla:

11.2.1.1.1 Tabla de clasificación de la probabilidad: Escenario 1

	Frecuencia de la Actividad - Probabilidad	Nivel de Exposición
Casi seguro	La actividad conlleva a que el riesgo se ejecute más de 5000 veces por año y al menos una vez en los últimos 4 meses se ha presentado la materialización.	**5 – 100%**
Probable	La actividad conlleva a que el riesgo se ejecute mínimo 500 veces al año y máximo 5000 veces por año y al menos una vez en los últimos 8 meses se ha presentado la materialización.	**4 – 80%**
Posible	La actividad conlleva a que el riesgo se ejecute 24 a 499 veces por año y al menos una vez en los últimos 12 meses se ha presentado la materialización.	**3 – 60%**
Imposible	La actividad conlleva a que el riesgo se ejecute de 3 a 23 veces por año y al menos una vez en los últimos 16 meses se ha presentado la materialización.	**2 – 40%**
Rara vez	La actividad conlleva a que el riesgo se ejecute como máximos 2 veces por año y nunca se ha presentado la materialización en los últimos 24 meses	**1 – 20%**

11.2.1.2 Escenario 2: Riesgo previamente identificado

En el segundo escenario, nos enfrentamos a un riesgo que ya se encuentra previamente identificado dentro de la matriz de riesgos institucional, por lo tanto, ha surtido cada una de las etapas de la administración de riesgos descritas en este documento y en consecuencia se tienen datos históricos frente a la efectividad en la administración, así como el número de materializaciones.

En este sentido, cuando se trata de este tipo de riesgos, el cálculo de la probabilidad inherente o residual se desarrollará basados en el número de materializaciones que ha tenido el riesgo en un periodo de tiempo. La selección para ese escenario se basará en la siguiente tabla:

11.2.1.2.1 Tabla de clasificación de la probabilidad: Escenario 2

	Frecuencia de la Actividad - Probabilidad	Nivel de Exposición
Casi seguro	Se ha materializado al menos una vez en los últimos 4 meses.	**5 – 100%**
Probable	Se ha materializado al menos una vez en los últimos 8 meses.	**4 – 80%**
Posible	Se ha materializado al menos una vez en los últimos 12 meses.	**3 – 60%**
Imposible	Se ha materializado al menos una vez en los últimos 16 meses. se ha presentado la materialización.	**2 – 40%**
Rara vez	No se ha materializado en los últimos 24 meses	**1 – 20%**

11.2.2 Clasificación del impacto inherente

Para la clasificación del impacto se consideran dos clases fundamentales que recogen en gran medida los impactos de tipo estratégico, de cumplimiento, tecnológicos, litigioso, etc. El primero es el económico, el cual, afecta la disponibilidad de recursos monetarios de CISA (multa, sanción o afectación del presupuesto) para el cumplimiento de su misión y sus objetivos institucionales. El segundo es el reputacional, el cual, afecta la credibilidad, confianza y percepción de los usuarios sobre CISA.

Para identificar el impacto y asignarlo al riesgo, debe primero ubicar en la siguiente tabla las consecuencias en la columna correspondiente al tipo de impacto y seleccionar el nivel que le represente el mayor impacto, pensando siempre en el peor escenario, en caso de que el riesgo se llegase a materializar siendo el criterio suficiente para la selección.

11.2.2.1 Tabla de clasificación del impacto riesgo operativo y continuidad del negocio

		Económica	Reputacional
1 – 20%	**Leve**	Afectación menor a 60 SMLMV	El riesgo afecta la imagen de algún área de la organización.

2 – 40%	**Menor**	Entre 61 y 150 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
3 – 60%	**Moderado**	Entre 151 y 300 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
4 – 80%	**Mayor**	Entre 301 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
5 – 100%	**Catastrófico**	Mayor a 501 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Por su parte, con respecto a los riesgos de corrupción, la evaluación del impacto del riesgo se realiza con base en las siguientes preguntas y el número de respuestas positivas.

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 tratamiento 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?		

11.2.2.2 Tabla de clasificación del impacto riesgo de corrupción

	Rangos de respuesta	Severidad
Moderado	Entre 1 y 5 preguntas afirmativas	**3 – 60%**

Mayor	Entre 6 y 11 preguntas afirmativas	**4 – 80%**
Catastrófico	Entre 12 y 19 preguntas afirmativas	**5 – 100%**

11.2.3 Medir el riesgo inherente

Determinar el resultado de la calificación según los criterios definidos anteriormente, los cuales establecen un grado de exposición al riesgo, de esta forma se define el riesgo inherente, para esto, se debe cruzar el resultado obtenido en la probabilidad e impacto y ubicarlo en la zona correspondiente obteniendo así el nivel de riesgo.

Es importante destacar, que se utilizará un solo mapa de calor para determinar la calificación de los diferentes tipos de riesgos, buscando la simplificación de la metodología, pero sin perder en ningún momento lo estricto de la evaluación en cada caso. Además, que los riesgos de corrupción en el análisis de impacto se realizarán teniendo en cuenta los niveles “moderado”, “mayor” y “catastrófico”, dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto “insignificante” y “menor”.

MAPA DE CALOR[9]

Probailidad	IMPACTO				
	Insignificante	Menor	Moderado	Mayor	Catastrófico
Casi seguro	A	A	A	A	E
Probable	M	M	A	A	E
Posible	M	M	M	A	E
Imposible	B	M	M	A	E
Rara vez	B	B	M	A	E

11.3 VALORAR EL RIESGO

En esta etapa se realiza la identificación, descripción y calificación de los controles relacionados con el riesgo previamente identificado, los cuales deben estar directamente relacionados con las causas y consecuencias identificadas para de este modo modificarlo, obteniendo como resultado el riesgo residual.

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.

9 Adaptado de la Guía para la administración del riesgo y el diseño de controles en Entidades públicas

Asignables	Tienen responsables definidos para su ejecución.

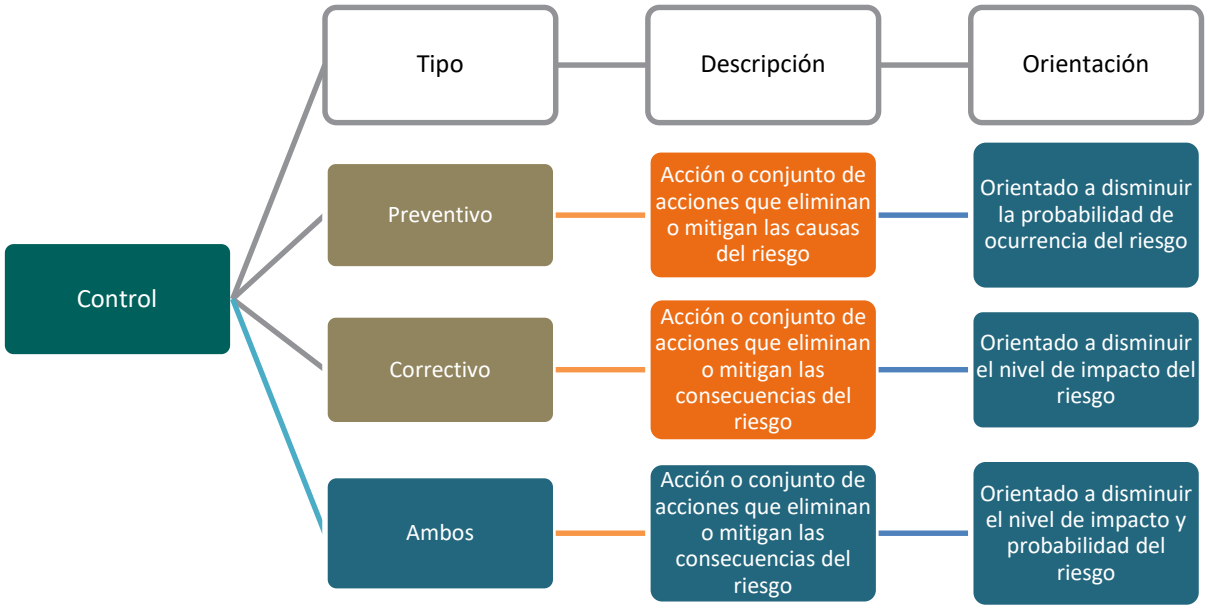
11.3.1 Identificar controles

Los controles son las acciones orientadas a modificar el riesgo[10] y que permiten determinar su tratamiento por parte de la entidad, puede ser minimizando la probabilidad de ocurrencia o el impacto del riesgo; la administración del riesgo contribuirá a la gestión de CISA en la medida en que los controles se identifiquen, documenten, apliquen y sean efectivos para prevenir o mitigar los riesgos. Es de este modo, previo a la determinación de la probabilidad e impacto del riesgo residual, se deben listar los controles existentes para administrar el riesgo identificado; este ejercicio permite conocer los mecanismos con los que se cuenta para controlar el riesgo, todo lo anterior deberá ser acorde con las condiciones reales de operación.

El listado de los controles se origina de los diferentes documentos con los que cuenta el proceso principalmente deberán ser tomados de los procedimientos (flujogramas), pero cuando se identifiquen controles que no estén debidamente documentados se listarán de igual manera para realizar su formulación, evaluación y formalización (numeral “Diseño de los Controles”).

11.3.1.1 Tipos de controles

Los controles se pueden clasificar en 2 tipos:



11.3.2 Diseño de los Controles

La evaluación de los controles consta de dos fases diseño y ejecución: la primera busca que los controles sean los suficientemente claros y específicos en cuanto a cómo se deberían realizar y, la segunda, tiene como

10 Guía para la administración del riesgo y el diseño de controles en entidades públicas

objetivo ejecutar de forma estandarizada los controles por los responsables establecidos en el diseño. Ambas fases deberán estar relacionadas, considerando que de nada sirve un control bien diseñado que no se ejecuta, o viceversa, un control que se ejecuta pero que no cumple con los parámetros de diseño, lo que conlleva a que puede aplicarse de maneras diferentes en su momento de ejecución, esto, sin lugar a duda, resultará en la ejecución inadecuada del mismo.

Dado lo anterior, es importante que para la administración de riesgos se efectué de forma adecuada la aplicación de controles, los cuales, contribuirán a la gestión de CISA, en la medida en que se identifiquen, documenten, apliquen y sean efectivos para prevenir o mitigar los riesgos identificados. A continuación, se describen 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 mitigar o reducir 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.

11.3.2.1 Evaluar los controles individualmente

La evaluación individual de cada uno de los controles asociados al riesgo se realiza con base en las fases descritas anteriormente de diseño y ejecución y 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	15	0

Fase	Factor	Orientación	Puntuación	
			Sí	No
		mismas permiten verificar, validar, cotejar, comparar o revisar el propósito del control?		
	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 anteriormente evaluados permitirán determinar la fortaleza del control en cada una de las fases, de este modo siempre que el puntaje del control sea menor a 96 puntos, el líder del proceso deberá implementar acciones orientadas a su mejoramiento, además, es posible que cada control mitigue una o más causas y consecuencias de acuerdo con su naturaleza. El resultado de la evaluación individual será a su vez un factor evaluado de manera grupal.
Adicionalmente, para mitigar los riesgos identificados en los procesos, hay causas que requieren documentar controles que pueden ser ejecutados por otras áreas o dependencias en razón a que un control puede mitigar una causa y un riesgo de un proceso, aunque éste no sea ejecutado por la misma área funcional.

Tenga en cuenta que, si los controles los ejecuta el personal de un proveedor, para que el control sea tenido en cuenta en la evaluación siguiente deberá estar incluido explícitamente en las cláusulas del contrato de este y enviada a la Gerencia de Planeación Estratégica la matriz de riesgos del proveedor correspondiente con el riesgo a evaluar.

11.3.2.2 Evaluar los controles grupalmente

Se calcula con base en el promedio de puntos obtenidos para cada uno de los controles analizados en la evaluación individual anterior; 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 mitigar la totalidad de las causas, de no ser así, se debe disminuir porcentualmente la calificación de acuerdo con la cantidad de causas descubiertas.

Ejemplo: si un riesgo tiene cinco (5) causas identificadas y se aplican cuatro (4) controles que solo mitigan a tres (3) de las causas, se tendría el siguiente resultado:

# 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		

Dado lo anterior se contempla, que para cada causa deberá existir un control. Las causas, deben ser descritas de forma clara, separada y no en conjunto (nido de causas); además, un control podrá ser tan eficiente que puede mitigar varias causas, en estos casos se repite el control, asociado de manera independiente a la causa específica.

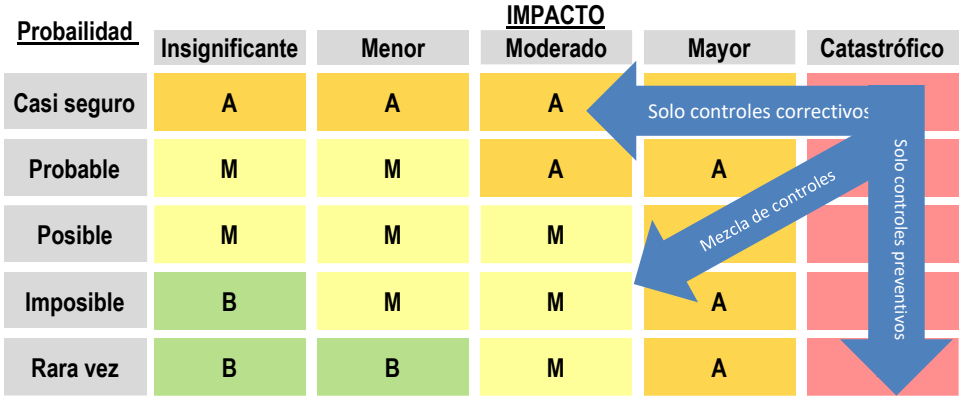
11.3.2.3 Medir el riesgo residual

Se entiende por riesgo residual el desplazamiento del riesgo inherente en su probabilidad o impacto resultante de calificar los controles para su administración.

Dado lo anterior se procede de la siguiente manera, partiendo del resultado de la determinación del riesgo inherente (Numeral "Clasificación del impacto inherente"), y la calificación grupal de los controles (Numeral "Evaluar los controles grupalmente"), lo cual permitirá modificar la calificación en el mapa de riesgo inherente, así:

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

De esta manera, el mapa de riesgo inherente disminuye su posición de la siguiente forma, obteniendo el nivel de riesgo.



Es importante resaltar, que la medición del riesgo residual se debe realizar de nuevo cuando haya un monitoreo de controles que, como consecuencia de la recalificación varié la calificación grupal anteriormente establecida, así como también cuando haya materializaciones sobre el riesgo.

Es importante resaltar que, para los riesgos estratégicos, podrán ser mitigados por controles o a través de las estrategias planteadas por CISA en el marco de la planeación estratégica, dichas estrategias pueden tener dos objetivos:

- Mitigar los efectos no deseados de la materialización de un riesgo.
- Aumentar los efectos deseados para el aprovechamiento de una oportunidad.

Las estrategias definidas se valoran bajo tres criterios, la estrategia mitiga impacto, probabilidad o ambas, así:

- De forma adecuada
- De forma moderada
- De forma débil

Bajo estos componentes los expertos valoran la mitigación de los riesgos estratégicos.

11.4 TRATAMIENTO (Manejo) DEL RIESGO

Se enfoca en el tratamiento que se debe dar al riesgo en el caso de identificar falta de controles en procesos, debilidades en los controles o materializaciones de los riesgos.

Cuando se ha determinado el riesgo residual, se toma esta ubicación como resultado, la cual se debe asociar la opción de manejo en la tabla siguiente, mediante la cual el líder del proceso le dará tratamiento:

	Zona de Riesgo	Opción de Manejo
B	Riesgo Bajo	Asumir el riesgo
M	Riesgo Moderado	Asumir el riesgo*
A	Riesgo Alto	Reducir el riesgo Evitar el riesgo Compartir o transferir el riesgo
E	Riesgo Extremo	Reducir el riesgo Evitar el riesgo Compartir o transferir el riesgo

Las estrategias de tratamiento sobre el riesgo 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 previamente relacionados.
  *Para los riesgos de corrupción en las zonas de "moderado con imposible", "moderado con posible", deberá tomar las acciones de reducir el riesgo.

- **Reducir el riesgo:** Tomar medidas encaminadas a disminuir ya sea la probabilidad (medidas de prevención) o el impacto (medidas de corrección).
  Ejemplo: optimización de procesos, definición de nuevos controles, entre otros.

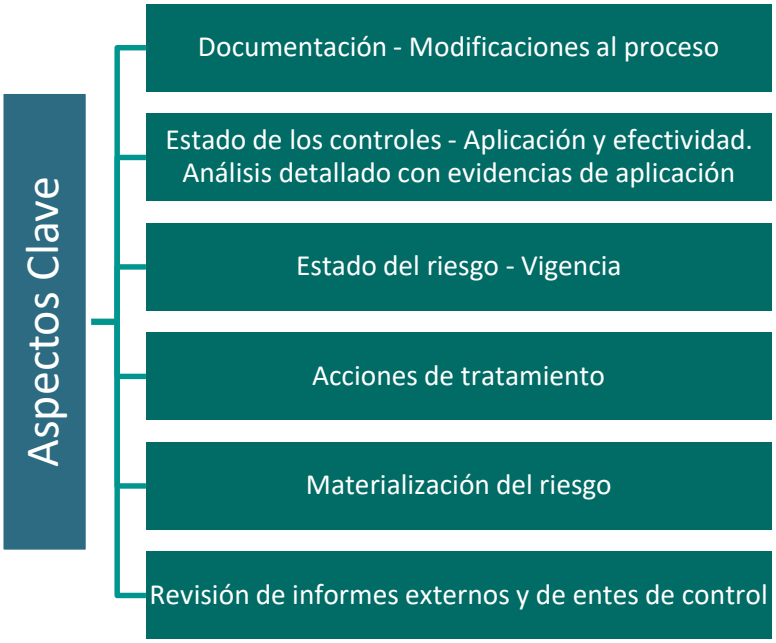
- **Evitar el riesgo:** Tomar las medidas encaminadas a eliminar el proceso o procedimiento que generan la existencia del riesgo y con ello la materialización del riesgo; para lo cual es necesario, al interior de los procesos generar cambios sustanciales por mejoramiento, rediseño o eliminación.
  Ejemplo: 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.
  Ejemplo: seguros, sitios alternos, contratos de riesgos compartidos, etc.

En caso de la opción elegida sea asumir el riesgo deberá monitorear según las instrucciones del numeral siguiente; pero si la opción es diferente a esta deberá formular las acciones orientadas a la creación y/o fortalecimiento de los controles cuando así se requiera, según el anexo "Plan de Tratamiento al Riesgo" el cual contiene como mínimo los campos: descripción del plan de acción, responsable, fecha de implementación y fecha de seguimiento, para cumplir las acciones correspondientes.

11.5 MONITOREAR Y REVISAR

Esta etapa dinamiza la gestión integral del riesgo, para lo cual se debe verificar el continuo 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 con una periodicidad de ejecución cuatrimestral (día 30 del mes de abril y día 31 de los meses agosto y diciembre), los procesos deben garantizar que se analizaron los siguientes aspectos:



Es por lo anterior que, se deben responder las siguientes preguntas, orientadas en acciones a desarrollar posteriormente:

Número	Pregunta	Respuesta	Etapa para 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 con 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 en ASE, una respuesta es negativa, es necesario actualizar los elementos del riesgo en la etapa respectiva describiendo exactamente lo sucedido, para esto es necesario informar a la Gerencia de Planeación Estratégica para analizar lo correspondiente.

Tenga en cuenta que a medida que los controles sean efectivos en el tiempo, es decir el riesgo no se materialice, la probabilidad se podrá disminuir paulatinamente en el riesgo residual 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, el líder del proceso podrá solicitar a la Gerencia de Planeación Estratégica la actualización la calificación del riesgo residual (aplica para los riesgos calculados bajo la probabilidad número de materializaciones).

11.5.1 Materialización del Riesgo

Las causales de materialización de riesgos operativos y continuidad del negocio:

La materialización del riesgo es uno de los temas de mayor impacto frente a la administración del riesgo, dado que se hace referencia a la afectación comprobada que se presenta sobre los objetivos estratégicos, del proceso o producto tras la ocurrencia de un evento.

Una materialización puede presentarse por alguno(s) de los siguientes motivos:

- No identificación del riesgo por parte del proceso y, por lo tanto, la no ejecución de controles para mitigarlo.
- Ocurrencia de una o varias de las causas asociadas al riesgo, acompañada de la falta de efectividad del control destinado para prevenirla.
- Falta de identificación de una causa asociada al riesgo, y, por lo tanto, falta de identificación de su respectivo control.
- Incumplimiento de la ejecución de alguno de los controles establecidos en los procedimientos descritos en el proceso.
- Causa externa previamente identificada sobre la cual CISA no pueda ejercer un control para prevenirla.
- Incumplimiento de un indicador de proceso relacionado con el riesgo.

11.5.1.1 Procedimiento de la materialización de riesgos operativos y continuidad del negocio

1. Identificación de la posible materialización de un riesgo

Existen dos fuentes por las cuales se podría identificar la posible materialización del riesgo:

- Por el líder del proceso o los integrantes de este, o;
- Por un tercero al proceso.

I. Procedimiento para la posible materialización de los riesgos de líder del proceso o los integrantes de este

2. Análisis de la posible materialización de un riesgo

El líder de proceso, en conjunto con sus colaboradores, es el responsable de determinar y dictaminar mediante un análisis exhaustivo la materialización del riesgo; en caso de ser necesario, el líder del proceso podrá solicitar colaboración de las diferentes áreas institucionales a fin de garantizar la agilidad y calidad de este proceso. La detección de la materialización del riesgo es una actividad que debe tener prioridad dentro

de la entidad; en caso de que el resultado sea negativo no tendrá que reportarlo, pero en el caso de que el resultado sea positivo deberá ejecutar el paso siguiente.

3. Determinación y reporte de la materialización

Producto del análisis y tan pronto como se determine que el resultado es positivo, se debe realizar el siguiente informe, que incluya la determinación de:

- ¿Que causó la 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?
- ¿Se realizó el análisis frente a la afectación de pólizas o reclamación de seguros que pudo causar la materialización del riesgo?
- ¿Se realizó el análisis frente a la afectación legal/acciones judiciales que pudo causar la materialización del riesgo?
- ¿La materialización del riesgo causo pérdidas económicas?
- ¿Cuánto fue el valor de las pérdidas económicas?

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. Es fundamental formular las acciones correctivas que fortalezcan el proceso.

Con respecto a lo mencionado anteriormente, se hace indispensable que la Alta Dirección esté enterada de los sucesos acontecidos, es por esto, que el líder de proceso deberá enviar a la Gerencia de Planeación Estratégica el informe consolidado, la evidencia del registro de la materialización en ASE y el anexo "Plan de Tratamiento al Riesgo" en un periodo no mayor a ocho (8) días calendario posterior a su detección.

A su vez, la Gerencia de Planeación Estratégica incluirá el informe sobre la materialización del riesgo en el siguiente Comité Institucional de Gestión y Desempeño Ordinario. Sin embargo, de ser necesario, el líder de proceso podrá solicita al Gerente de Planeación Estratégica, como secretario del Comité, que convoque a un Comité extraordinario para analizar la situación de la materialización.

II. Procedimiento para la posible materialización de los riesgos por parte de un tercero

2. Análisis de la posible materialización de un riesgo

Con el fin de garantizar que a nivel institucional se realice un seguimiento permanente a los sucesos que puedan conllevar a la materialización de los riesgos, las personas externas al proceso (Auditoría Interna, Auditoría Externa, Colaborador Interno u otro) una vez conozcan de algún hecho que a su juicio pueda

conllevar a la materialización, y por ende poner en riesgo el cumplimiento de alguno de los objetivos institucionales, deberán reportarlos a la Gerencia de Planeación Estratégica de forma clara y concreta.
En caso de presentarse esta situación, la Gerencia de Planeación Estratégica deberá citar al presidente de CISA en un plazo no mayor a ocho (8) días hábiles, con el fin de que determine un equipo interdisciplinario encargado de adelantar el análisis correspondiente sobre los hechos informados, deberá seleccionar como mínimo tres representantes de procesos diferentes. Independientemente del grupo interdisciplinario formado el análisis debe ser adelantado en el plazo que fije esta instancia dependiendo de las obligaciones de los involucrados.

3. Determinación y reporte de la materialización

Por su parte, en caso de que el análisis realizado por el grupo interdisciplinario establezca que se presentó la materialización del riesgo, debe generar y enviar a la Gerencia de Planeación Estratégica un informe con las evidencias correspondientes y la respuesta de las siguientes preguntas:

- ¿Que causó la 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?
- ¿Quiénes están implicados en la materialización del riesgo?
- ¿Se realizó el análisis frente a la afectación de pólizas o reclamación de seguros que pudo causar la materialización del riesgo?
- ¿Se realizó el análisis frente a la afectación legal/acciones judiciales que pudo causar la materialización del riesgo?
- ¿La materialización del riesgo causo pérdidas económicas?
- ¿Cuánto fue el valor de las pérdidas económicas?

A su vez, la Gerencia de Planeación Estratégica remitirá el informe al líder del proceso correspondiente. El líder deberá registrar la materialización del riesgo en ASE y en periodo no mayor a ocho (8) días calendario posterior a la solicitud realizada deberá enviar a la Gerencia de Planeación Estratégica el registro de la materialización en ASE, el anexo "Plan de Tratamiento al Riesgo" y la respuesta a las siguientes preguntas:

- ¿Qué acciones se deben realizar para reestablecer el curso de acción del proceso?
- ¿Qué actividades se deben desarrollar para fortalecer los controles?
- ¿Se realizó el análisis frente a la afectación legal/acciones judiciales que pudo causar la materialización del riesgo?

En caso de la no materialización del riesgo, el equipo interdisciplinario asignado deberá enviar el reporte directamente a la Gerencia de Planeación Estratégica.
A su vez, la Gerencia de Planeación Estratégica incluirá el informe sobre la materialización, o no, del riesgo según corresponda en el siguiente Comité Institucional de Gestión y Desempeño. Sin embargo, de ser necesario el Gerente de Planeación Estratégica podrá convocar a un Comité extraordinario para analizar la situación.

11.5.1.2 Procedimiento para realizar la materialización riesgos de corrupción

1. Identificación de posibles actos de corrupción

El reporte lo deberá realizar el líder del proceso, los integrantes de este, Auditoría Interna, Auditoría Externa, Colaborador Interno o Ciudadanía en General o cualquier otro tercero que tenga conocimiento sobre posibles actos de corrupción llevados a cabo dentro de CISA. El reporte deberá ser realizado por medio de los canales dispuestos para tal fin, los cuales se describen en el Memorando Circular 046 “Política para la Prevención de Corrupción y Procedimiento para la Gestión de Reportes de Actos de Corrupción” para que se agote el respectivo procedimiento.

2. Análisis del impacto del posible acto de corrupción

Cuando el Comité de Ética defina cuales sucesos acontecidos deban ser puestos en conocimiento por la Gerencia de Planeación Estratégica con el fin de analizar una posible materialización de un riesgo de corrupción, la oficial de Transparencia los informará. A su vez, esta Gerencia, analizará la información y determinará en que proceso y sobre qué riesgo actual se puede presentar la afectación.

3. Planear y realizar acciones

La Gerencia de Planeación Estratégica deberá realizar un análisis de los acontecimientos haciendo énfasis sobre las siguientes preguntas:

- ¿Qué posibilitó la generación del posible hecho de corrupción?
- ¿Qué control es susceptible de mejora para prevenir la posibilidad de ocurrencia de las causas relacionadas con el posible acto de corrupción?
- ¿Qué acciones se deben adelantar para fortalecer los controles?

Se hace indispensable que la Alta Dirección esté enterada de los sucesos acontecidos, por ello, la Gerencia de Planeación Estratégica deberá realizar una presentación sobre este análisis y un plan de mejora sobre las causas identificadas al presidente y vicepresidente del proceso.

4. Materialización del riesgo de corrupción

Se entenderá materializado el riesgo una vez los entes externos o funcionarios internos encargados competentes de realizar la investigación determinen que existió un acto de corrupción comprobado dentro de CISA. Dicha decisión debe ser informada a la Gerencia de Planeación Estratégica quien, a su vez, solicitara al líder del proceso un informe en el que se incluya la evidencia del registro de la materialización en ASE, el anexo “Plan de Tratamiento al Riesgo” y las respuestas de las siguientes preguntas:

- ¿Que causó la 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 actividades se deben desarrollar para fortalecer los controles?
- ¿Quiénes están implicados en la materialización del riesgo?
- ¿Se realizó el análisis frente a la afectación de pólizas o reclamación de seguros que pudo causar la materialización del riesgo?
- ¿Se realizó el análisis frente a la afectación legal/acciones judiciales que pudo causar la materialización del riesgo?
- ¿La materialización del riesgo causo pérdidas económicas?
- ¿Cuánto fue el valor de las pérdidas económicas?

El informe descrito sobre la materialización del riesgo deberá ser enviado a la Gerencia de Planeación Estratégica en un periodo no mayor a ocho (8) días calendario posterior a la comunicación, el cual será incluido en el siguiente Comité Institucional de Gestión y Desempeño; sin embargo, el Gerente de Planeación Estratégica podrá convocar a un Comité extraordinario para analizar la situación de la materialización de ser necesario.

11.5.2 Gestión de eventos

Un evento es un riesgo materializado se puede considerar como los incidentes que generan o podrían generar pérdidas futuras a CISA. Cada vez que se reporten eventos comprobados de esta naturaleza por parte de cualquier fuente, la Gerencia de Planeación Estratégica verificará que el líder del proceso haya realizado el registro correspondiente en ASE en caso de aplicar, para así obtener la base de eventos actualizada y con ello realizar el seguimiento respectivo, en aras de ejecutar lo establecido en la presente circular normativa.

11.5.3 Indicadores

Son una colección de datos históricos por periodos de tiempo relacionados con el cumplimiento del objetivo del proceso. De acuerdo con los indicadores actualmente existentes, el líder del proceso deberá diligenciar el registro de indicadores del SIG anexo “Formato Registro de Indicadores de Proceso” perteneciente al manual 13 “Manual del SIG” en las fechas establecidas para ello, pero, en caso de que el indicador no haya cumplido la meta deberá analizar y contestar la siguiente pregunta ¿el incumplimiento del indicador generó la materialización de un riesgo del proceso? En caso de responder sí, deberá ejecutar lo descrito en el ítem Materialización del riesgo del presente documento, dado que esto puede indicar al líder del proceso alguna desviación sobre el objetivo.

12. MAPA DE RIESGOS

Como producto de la aplicación de la metodología anterior se obtendrán los mapas de riesgo. 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:

12.1 Mapa de riesgos institucionales

Este mapa construye 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.
- ✓ Son clasificados como riesgos de continuidad del negocio.

12.2 Mapa de Riesgos de Corrupción

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

12.3 Mapa de Riesgos Operativos

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

12.4 Mapa de riesgos de continuidad del negocio

Este mapa construye aquellos riesgos que fueron clasificados dentro de la etapa de identificación general como “Riesgos Continuidad del Negocio”.

12.5 Mapa de riesgos consolidado

Integra la totalidad de los riesgos de la Entidad.

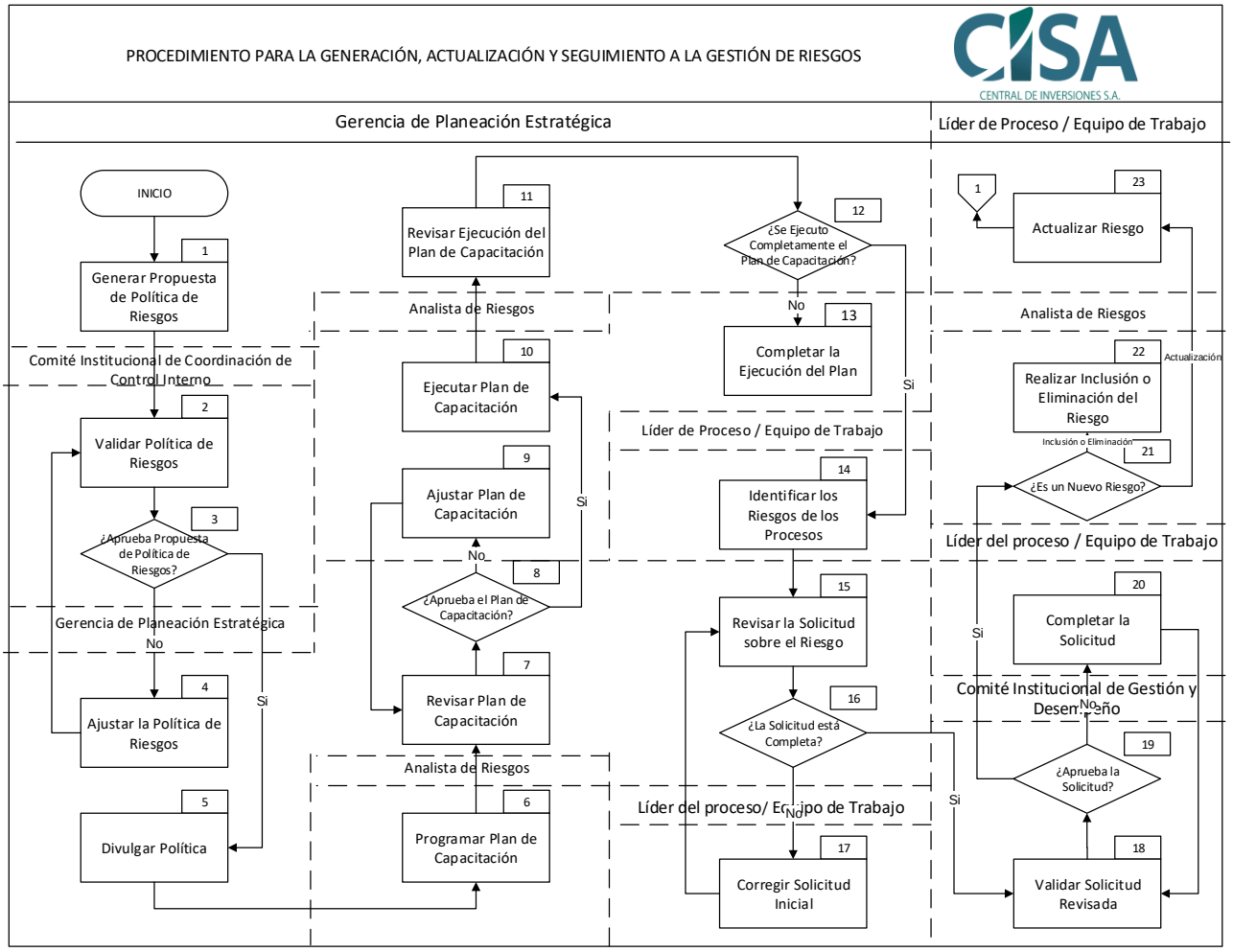
13. POSIBLES SANCIONES POR INCUMPLIMIENTO A LA POLÍTICA DISPUESTA PARA LA ADMINISTRACIÓN DEL RIESGO

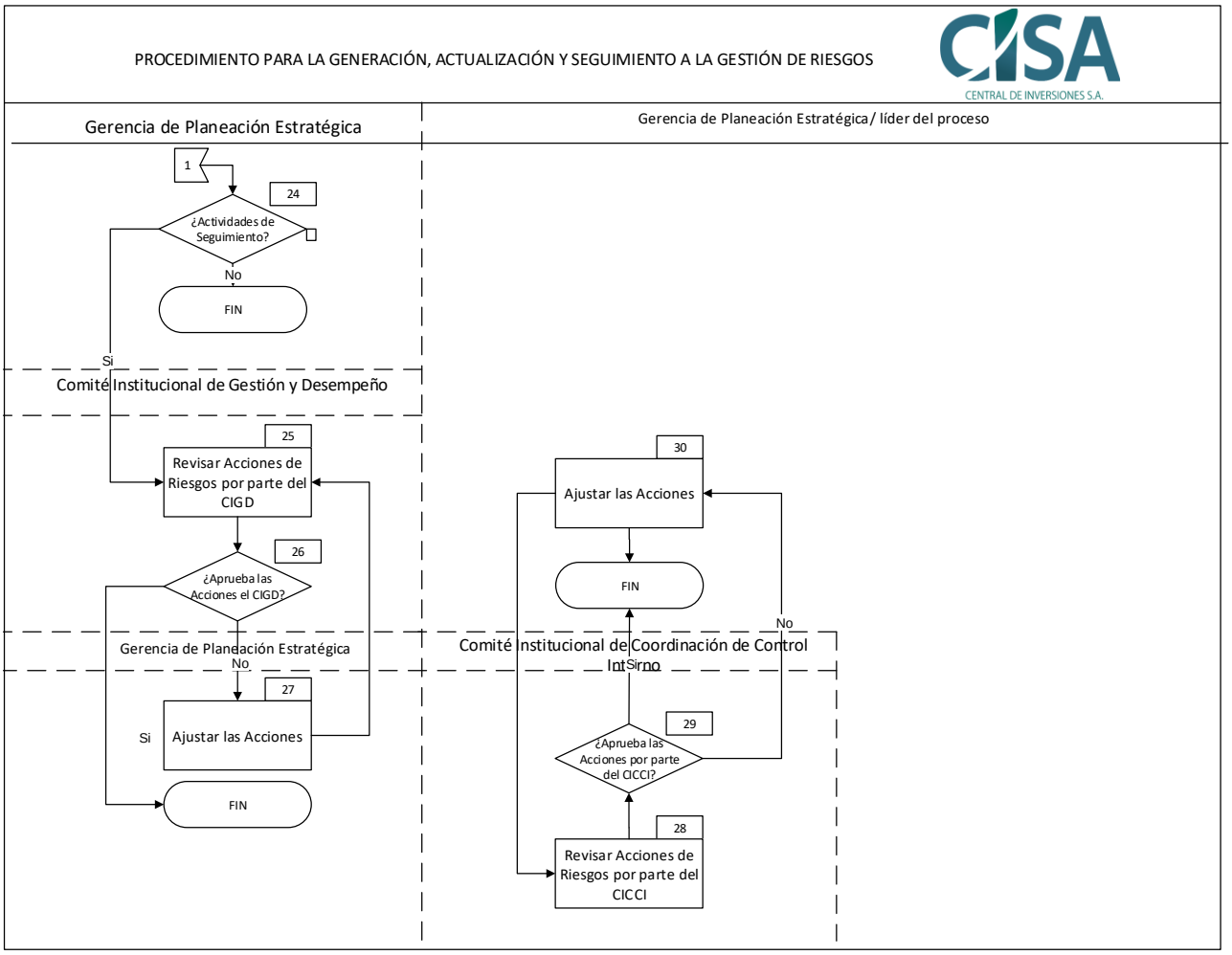
Todos empleados de CISA tienen la obligación institucional de cumplir con la totalidad de los lineamientos, directrices, obligaciones y procedimientos contenidos en la presente política sus partes y anexos. Se entenderá que el no hacerlo expone a CISA a riesgos legales, de reputación, financieros, operativos, entre otros.

El incumplimiento a esta política podrá dar lugar a procesos disciplinarios de orden laboral sin perjuicio de las acciones disciplinarias a las que haya lugar de acuerdo con lo previsto en el Código disciplinario único/general o la que la remplace.

14. PROCEDIMIENTO PARA LA GENERACIÓN, ACTUALIZACIÓN Y SEGUIMIENTO A LA GESTIÓN DE RIESGO

DIAGRAMA DE PROCESOS





DESCRIPCIÓN DETALLADA

No.	Actividad	Descripción de la Actividad	Responsable	Registro
1	**Generar Propuesta de Política de Riesgos**	Proponer y actualizar la política de administración del riesgo con su respectiva metodología (nuevas versiones a la misma), tomando como referencia los lineamientos del Gobierno Nacional y las prácticas internacionales en materia de gestión del riesgo.	Gerencia de Planeación Estratégica	Documento con propuesta de política
2	**Validar Política de Riesgos**	El Comité Institucional de Coordinación de Control Interno, evaluará por lo menos una vez en el año la pertinencia de la propuesta presentada correspondiente con la revisión a	Comité Institucional de Coordinación de Control Interno	Acta de Comité

No.	Actividad	Descripción de la Actividad	Responsable	Registro
		adelantar en el marco del Plan Anticorrupción y Atención al Ciudadano). En caso de requerirse generará las observaciones que considere necesarias.		
3	**¿Aprueba Propuesta de Política de Riesgos?**	**Si la respuesta es Afirmativa, pasa a la Actividad No. 5.** **Si la respuesta es Negativa, pasa a la actividad No. 4.**	Comité Institucional de Coordinación de Control Interno	
4	**Ajustar la Política de Riesgos**	Realizar las modificaciones, dentro de los plazos establecidos, para presentar nuevamente al Comité Institucional de Coordinación de Control Interno. **Pasa a la actividad No. 2.**	Gerencia de Planeación Estratégica	Documento con propuesta de política ajustada
5	**Divulgar Política**	Divulgar los lineamientos impartidos en la política aprobada, para lo cual podrá utilizar diferentes medios (boletines, capacitaciones, correos, etc.). Se entenderá por divulgadas las actualizaciones enviadas por medio del correo electrónico del Sistema Integrado de Gestión.	Gerencia de Planeación Estratégica	Correo Electrónico del SIG "Actualización de documentos".
6	**Programar Plan de Capacitación**	Anualmente, se deberá programar un plan de capacitación para toda la Entidad respecto de la metodología (a quienes apliquen), de los conceptos y materia de riesgos.	Analista de Riesgos	Plan de capacitación
7	**Revisar Plan de Capacitación**	El Gerente de Planeación Estratégica, deberá revisar que el plan de capacitación propuesto contemple el alcance pertinente y el contenido preciso para lograr el objetivo de estas.	Gerencia de Planeación Estratégica	Correo Electrónico
8	**¿Aprueba el Plan de Capacitación?**	**Si la respuesta es Afirmativa, pasa a la actividad No. 10.** **Si la respuesta es Negativa, pasa a la actividad No. 9.**	Gerencia de Planeación Estratégica	
9	**Ajustar Plan de Capacitación**	Realizar las modificaciones y/o ajustes solicitados de acuerdo con lo establecido, para posteriormente enviar por correo electrónico al Gerente de Planeación Estratégica.	Analista de Riesgos	Correo Electrónico

No.	Actividad	Descripción de la Actividad	Responsable	Registro
		Pasa a la actividad No. 7.		
10	**Ejecutar Plan de Capacitación**	Ejecutar el plan de capacitación en las fechas correspondientes dejando como evidencia los listados de asistencia, así como las presentaciones; una vez finalizadas las actividades deberá consolidar la información y remitir por correo electrónico al Gerente de Planeación Estratégica la novedad.	Analista de Riesgos	Listado de asistencia / Presentación / Correo electrónico
11	**Revisar Ejecución del Plan de Capacitación**	Una vez reciba el correo, deberá revisar la ejecución del plan de capacitación de acuerdo con las evidencias remitidas.	Gerencia de Planeación Estratégica	Correo Electrónico
12	**¿Se Ejecuto Completamente el Plan de Capacitación?**	**Si la respuesta es Afirmativa, pasa a la actividad No. 14.** **Si la respuesta es Negativa, pasa a la actividad No. 13.**	Gerencia de Planeación Estratégica	
13	**Completar la Ejecución del Plan**	Revisar lo faltante y programar lo que corresponda, para posteriormente completar las evidencias de la ejecución y enviar por correo electrónico al Gerente de planeación estratégica. **Pasa a la actividad No. 11.**	Analista de Riesgos	Listado de asistencia / Presentación / Correo electrónico
14	**Identificar los Riesgos de los Procesos**	El líder de proceso junto con su equipo de trabajo deberá identificar, actualizar y/o eliminar riesgos de acuerdo con los lineamientos impartidos en la presente política, determinando las causas fuentes del riesgo y los eventos con base al contexto de la Entidad y del proceso, que pudieren afectar el logro de los objetivos. Para lo cual, podrá convocar a la Gerencia de Planeación Estratégica quienes brindarán un acompañamiento metodológico para la correcta definición y/o actualización de los riesgos. En caso de los riesgos nuevos, se deberá diligenciar el anexo "Ficha técnica para el levantamiento de riesgos (Matriz de Riesgos)".	Líder de Proceso / Equipo de Trabajo	Mapa de Riesgos

No.	Actividad	Descripción de la Actividad	Responsable	Registro
15	**Revisar la Solicitud sobre el Riesgo**	Cada vez que se presente por parte de un líder de proceso la solicitud, la Gerencia de Planeación estratégica revisara que esté de acuerdo con lo establecido en la presente circular normativa.	Gerencia de Planeación Estratégica / Analista de Riesgos	Correo Electrónico
16	**¿La Solicitud está Completa?**	**Si la respuesta es Afirmativa, pasa a la Actividad No. 18.** **Si la respuesta es Negativa, pasa a la Actividad No. 17.**	Gerencia de Planeación Estratégica / Analista de Riesgos	
17	**Corregir Solicitud Inicial**	Conforme las observaciones se proceden a revisar lo faltante y/o modificar lo que corresponda y enviar por correo electrónico al Gerente de Planeación Estratégica y/o Analista de Riesgos para revisión. **Pasa a la actividad No. 15.**	Líder del proceso / Equipo de Trabajo	Correo electrónico
18	**Validar Solicitud Revisada**	Cada vez que sea presentada una solicitud de riesgos por parte de la Gerencia de Planeación Estratégica, el Comité Institucional de Gestión y Desempeño validará la pertinencia de su inclusión, modificación o eliminación del riesgo de acuerdo con los objetivos del proceso en mención.	Comité Institucional de Gestión y Desempeño	Acta de Comité
19	**¿Aprueba la Solicitud?**	**Si la respuesta es Afirmativa, pasa a la Actividad No. 21.** **Si la respuesta es Negativa, pasa a la Actividad No. 20.**	Comité Institucional de Gestión y Desempeño	
20	**Completar la Solicitud**	Realizar ajustes y presentar la modificación nuevamente al Comité Institucional de Gestión y Desempeño para su respectiva aprobación. **Pasa a la actividad No. 18.**	Líder del proceso / Equipo de Trabajo	Correo electrónico
21	**¿Es un Nuevo Riesgo?**	**Si la respuesta es una Inclusión o Eliminación de un riesgo, pasa a la Actividad No. 22.** **Si la respuesta es una Actualización de un riesgo, pasa a la Actividad No. 23.**	Analista de Riesgos	

No.	Actividad	Descripción de la Actividad	Responsable	Registro
22	**Realizar Inclusión o Eliminación del Riesgo**	Realizar la inclusión o eliminación del riesgo en el Aplicativo de Seguimiento a la Estrategia – ASE, según corresponda la solicitud, del cual, se constituye en el sistema informático en el cual reposará la información relativa a los riesgos (Operativos, Corrupción y Continuidad del Negocio).	Analista de Riesgos	Reporte del Aplicativo de Seguimiento a la Estrategia – ASE
23	**Actualizar Riesgo**	Realizar la actualización del riesgo en el Aplicativo de Seguimiento a la Estrategia – ASE, según corresponda la solicitud, del cual, se constituye en el sistema informático en el cual reposará la información relativa a los riesgos (Operativos, Corrupción y Continuidad del Negocio).	Líder de Proceso / Equipo de Trabajo	Reporte del Aplicativo de Seguimiento a la Estrategia – ASE
		ACTIVIDADES DE SEGUIMIENTO		
24	**¿Actividades de Seguimiento?**	**Si la respuesta es Afirmativa, pasa a la actividad No. 25.** **Si la respuesta es Negativa, FIN.**	Gerencia de Planeación Estratégica	
25	**Revisar Acciones de Riesgos por parte del CIGD**	Cada vez que se requiera la Gerencia de Planeación Estratégica comunicara las novedades frente materializaciones, monitoreos, planes de tratamiento del riesgo, actualizaciones, resultado de apetito del riesgo y capacidad, al Comité Institucional de Gestión y Desempeño para que sea revisado, y evaluadas las acciones, de acuerdo con la metodología descrita en el presente documento.	Comité Institucional de Gestión y Desempeño	Acta de comité
26	**¿Aprueba las Acciones el CIGD?**	**Si la respuesta es Afirmativa, FIN.** **Si la respuesta es Negativa, pasa a la actividad No. 27.**	Comité Institucional de Gestión y Desempeño	
27	**Ajustar las Acciones**	Realizar las modificaciones y/o ajustes solicitados para posteriormente presentar en el siguiente Comité. **Pasa a la Actividad No. 25.**	Gerencia de Planeación Estratégica	Correo Electrónico
28	**Revisar Acciones de Riesgos por parte del CICCI**	Trimestralmente la Gerencia de Planeación Estratégica comunicara las novedades frente materializaciones, monitoreos, planes de tratamiento del	Comité Institucional de Coordinación	Actas de Comité

No.	Actividad	Descripción de la Actividad	Responsable	Registro
		riesgo, actualizaciones al Comité Institucional de Coordinación de Control Interno para que sea revisado, y evaluadas las acciones de acuerdo con la metodología descrita en el presente documento.	de Control Interno	
29	**¿Aprueba las Acciones por parte del CICCI?**	**Si la respuesta es Afirmativa, FIN.** **Si la respuesta es Negativa, pasa a la actividad No. 30.**	Comité Institucional de Coordinación de Control Interno	
30	**Ajustar las Acciones**	Realizar las modificaciones y/o ajustes a las observaciones o sugerencias, el líder de proceso será el encargado de materializarlas. **Pasa a la actividad No. 28**	Gerencia de Planeación Estratégica / líder del proceso	Correo Electrónico

15. ANEXOS

ANEXO No. 1	Ficha técnica para el levantamiento de riesgos (Matriz de Riesgos)
ANEXO No. 2	Instructivo para la Gestión de Riesgos para Activos de Información
ANEXO No. 3	Plan de Tratamiento al Riesgo
ANEXO No. 4	Instructivo para el Monitoreo de Riesgos en el Aplicativo de Seguimiento a la Estrategia – ASE

16. 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.
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.

Versión	Fecha	Motivo de la Revisión	Modificaciones
			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 “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”

Versión	Fecha	Motivo de la Revisión	Modificaciones
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.” 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

Versión	Fecha	Motivo de la Revisión	Modificaciones
			"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 "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

Versión	Fecha	Motivo de la Revisión	Modificaciones
			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 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"
17	Diciembre 23 de 2019	Actualización del documento – Creación riesgos de continuidad del Negocio.	Se modificaron los numerales 3 "Alcance", 4 "Responsables", 6 "Normatividad Legal Aplicable", 9.1.7 "Clasificación de los riesgos", 10.1 "Mapa de riesgos institucionales" y 11 "Instructivo para el Monitoreo de Riesgos en el Aplicativo de Seguimiento a la Estrategia – ASE".

Versión	Fecha	Motivo de la Revisión	Modificaciones
			Se creó el numeral 10.4 “Mapa de riesgos de continuidad del negocio”. Se creó el anexo No. 3 “Instructivo para la Gestión de Riesgos de Continuidad del Negocio”. Se cambió en todo el cuerpo de la circular el nombre de la Gerencia de Planeación Estratégica y Proyectos por la Gerencia de Planeación Estratégica, conforme a la nueva estructura aprobada por Junta Directiva el 25 de noviembre del 2019.
18	Marzo 25 de 2020	Mejora del proceso	Del numeral 9.2.2. “Calificación del Riesgo”, se modificó la “Tabla de Clasificación del Impacto”. Se creó el numeral 12 “Procedimiento para la Generación y Actualización de Mapa de Riesgos”.
19	Mayo 06 de 2020	Mejora del proceso	Se ajustó la redacción de los numerales de la Circular Normativa para facilitar la comprensión de la Política de administración del riesgo en Central de Inversiones S.A.
20	Mayo 13 de 2020	Mejora del proceso	Se modificó el numeral 9.5.1 “Materialización del Riesgo”.
21	Septiembre 02 de 2020	Mejora del proceso / Metodología para el diseño y documentación de controles del proceso.	Se ejecutaron actualizaciones de forma y numeración en todo el cuerpo de la circular normativa, con el fin de mejorar su lectura y comprensión. Se modificaron los numerales 4 “Responsables”, 5. “Términos y Definiciones”, 9.5.1 “Materialización del Riesgo” y 12.” Procedimiento para la Generación y Actualización de Mapa de Riesgos”
22	Diciembre 18 de 2020	Actualización del documento.	Se modificó la Circular Normativa y sus anexos, teniendo en cuenta la actualización de la nueva imagen corporativa y la nueva denominación de las Oficinas Zona.
23	Julio 19 de 2021	Actualización del documento / Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas V.5	Se modificó todo el cuerpo de la circular normativa teniendo en cuenta los lineamientos establecidos en la Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas V.5 emitida por el Departamento Administrativo de la Función Pública (DAFP).

Versión	Fecha	Motivo de la Revisión	Modificaciones
			Se modificó el anexo No. 1 “Ficha técnica para el levantamiento de riesgos (Matriz de Riesgos)”. Se eliminó el anexo No. 3 “Instructivo para la Gestión de Riesgos de Continuidad del Negocio”. Se crearon los anexos No. 3 “Plan de Tratamiento al Riesgo” y 4. “Instructivo para el Monitoreo de Riesgos en el Aplicativo de Seguimiento a la Estrategia – ASE”.
24	Septiembre 02 de 2021	Mejora del proceso – Actualización clasificación activos de información	Se actualizó la clasificación de Seguridad de la Información de la Circular Normativa. Se actualizó la clasificación de Seguridad de la Información de los anexos No. 2 “Instructivo para la Gestión de Riesgos de Seguridad Digital” y No 3. “Plan de Tratamiento al Riesgo”.