CONTENIDO

1. DECLARACIÓN DE LA POLÍTICA DE ADMINISTRACIÓN DE RIESGOS 3
2. OBJETIVO 3
3. ALCANCE 4
4. ALINEACIÓN ESTRATÉGICA 4
5. RESPONSABLES 4
6. INSTITUCIONALIDAD 7
7. NORMATIVIDAD LEGAL Y APLICABLE 8
8. MARCO CONCEPTUAL DEL APETITO DE RIESGO 8
8.1 Comunicación marco integral de apetito de riesgo 9
8.2 Declaración del apetito del riesgo 9
9. ESTABLECIMIENTO DEL CONTEXTO INSTITUCIONAL 9
9.1 Establecimiento del contexto interno 10
9.2 Establecimiento del contexto externo 11
10. CLASES DE RIESGOS ADMINISTRADOS 12
11. METODOLOGÍA GENERAL PARA LA ADMINISTRACIÓN DE RIESGOS 13
IDENTIFICAR EL RIESGO 13
11.1 13
11.1.1 Describir la posible materialización del riesgo 13
11.2 ANALIZAR EL RIESGO 14
11.3 VALORAR EL RIESGO 14
11.4 TRATAMIENTO - MANEJO DEL RIESGO 15
11.5 MONITOREAR Y REVISAR 15
11.5.1 Materialización del Riesgo 15
11.5.2 Gestión de eventos 16
11.5.3 Indicadores 16
12. POSIBLES SANCIONES POR INCUMPLIMIENTO A LA POLÍTICA DISPUESTA PARA LA ADMINISTRACIÓN DEL RIESGO 16
13. ANEXOS 17

14. CONTROL DE CAMBIOS 17

Revisó	Aprobó
DIRECTOR DE PLANEACIÓN ESTRATÉGICA Y SISTEMAS DE INFORMACIÓN	DIRECTOR DE PLANEACIÓN ESTRATÉGICA Y SISTEMAS DE INFORMACIÓN
19/07/2024	19/07/2024

1. DECLARACIÓN DE LA POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

Con base en el Modelo Integrado de Planeación, y Gestión – MIPG específicamente la Dimensión de Direccionamiento estratégico y Planeación, y la Política de Planeación Institucional, se dan las directrices para establecer una política de riesgos alineada con los objetivos estratégicos y con la metodología *de la Guía para la administración del riesgo y el diseño de controles en entidades públicas*, emitida por el Departamento Administrativo de la Función Pública y en la ISO 31000 para identificar, analizar, valorar y tratar los riesgos de la entidad permitiendo tomar decisiones adecuadas y fijar lineamientos que serán transmitidos y liderados por la alta Dirección.

En CISA la administración del riesgo es fundamental para lograr los objetivos institucionales en el marco del compromiso con la gestión transparente y el cumplimiento de los valores institucionales. La entidad reconoce que, en el desarrollo de sus actividades se generan riesgos inherentes en los diferentes procesos. Por esta razón, CISA se compromete a definir y aplicar medidas para detectarlos, prevenirlos y corregir las desviaciones que se presenten, que puedan afectar los objetivos, mediante la adopción de los mecanismos y acciones necesarias para darles el tratamiento adecuado, identificando, analizando, valorando y monitoreando 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.

2. OBJETIVO

Definir lineamientos para la administración del riesgo y un marco metodológico para la gestión de los riesgos estratégicos, operativos, fiscales, de seguridad digital, continuidad del negocio, lavado de activos, financiación del terrorismo, financiación de la proliferación de armas de destrucción masiva, violación al régimen de la libre competencia económica, salud y seguridad en el trabajo, y corrupción de CISA, orientada a monitorearlos y revisarlos, con el fin de minimizar su ocurrencia y mitigar el impacto ante una eventual materialización; se articula con las demás políticas y planes contribuyendo al desempeño, y a la consecución de los objetivos estratégicos y de los procesos, asegurando razonablemente el alcance de las metas institucionales.

Igualmente, esta política busca promover la mejora continua en los procesos en toma de decisiones, teniendo en cuenta los siguientes lineamientos:

- 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, asegurando la eficacia y eficiencia.
- Gestionar de forma anticipada las vulnerabilidades o eventos que puedan afectar el logro de los objetivos institucionales.

3. ALCANCE

Esta política contempla los riesgos operativos, fiscales, lavado de activos, financiación del terrorismo, financiación de la proliferación de armas de destrucción masiva, violación al régimen de la libre competencia económica, continuidad del negocio, corrupción, estratégicos (ver anexo), de seguridad digital (ver anexo) y de salud y seguridad en el trabajo (ver anexos) relacionados con los procesos que ejecuta CISA, además de cada una de sus agencias. No contempla los riesgos asociados a la gestión ambiental toda vez que se trata en normativas diferentes.

4. ALINEACIÓN ESTRATÉGICA

Esta política se encuentra alineada y aporta a logro de los pilares definidos en el Plan Estratégico 2023-2026, específicamente con el lineamiento estratégico de operar con transparencia.

5. RESPONSABLES

Asegurando que las responsabilidades para la gestión del riesgo, se asignen y se comuniquen a los roles pertinentes, CISA determinó lo siguiente de acuerdo con sus líneas de defensa.

LÍNEA ESTRATÉGICA - ALTA DIRECCIÓN, COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO Y COORDINACIÓN DE CONTROL INTERNO:

- Revisar y analizar las propuestas presentadas por la Dirección de Planeación Estratégica y Sistemas de Información sobre la Política de Administración del Riesgo para la implementación en CISA y aprobarla.
- 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 analizando la gestión del riesgo.
- Aprobar el marco del apetito de riesgo para CISA y asegurar que sea coherente con los objetivos estratégicos establecidos, 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 (riesgos críticos) 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.
- Aprobar los riesgos relacionados con la continuidad del negocio.
- Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción, correspondiente a los riesgos de seguridad digital.

- Establecer, revisar y aprobar el contexto institucional (interno y externo)

PRIMERA LÍNEA DE DEFENSA - LÍDERES DE PROCESO, EQUIPO OPERATIVO INCLUIDOS TODOS LOS SERVIDORES: Responsables de gestionar los riesgos y hacer seguimiento en 1ª línea. El equipo operativo debe servir de enlace directo entre el proceso y la Dirección de Planeación Estratégica y Sistemas de Información para asegurar la aplicación de las metodologías aquí desarrolladas.

- Apoyar la construcción del contexto institucional (interno y externo), así como de definir las partes interesadas para su proceso.
- Validar 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 (Mapa de Riesgos)", solo aplica para los riesgos nuevos.
- Identificar los cambios en el proceso y actualizar el mapa de riesgos y la documentación de los controles, por lo menos una vez al año y enviar a la Dirección de Planeación Estratégica y Sistemas de Información las novedades presentadas para modificar lo correspondiente en el aplicativo.
- Lideres de los procesos, divulgar a todos los servidores del proceso el mapa de riesgos correspondiente, incluyendo las agencias.
- Realizar monitoreo de los riesgos del proceso a través del Aplicativo de Seguimiento a la Estrategia (ASE).
- Diseñar y ejecutar los controles, asegurar su correcta documentación, aplicación, fortalecimiento e implementación de acciones de tratamiento sobre el riesgo.
- Registrar el monitoreo de los riesgos del proceso a través del aplicativo correspondiente, de acuerdo con la periodicidad en adelante señalada.
- En caso de su eventual materialización, seguir lo mencionado en el ítem "Materialización del Riesgo" y reportar a la Dirección de Planeación Estratégica y Sistemas de Información.
- El equipo operativo debe servir de enlace directo entre el proceso y la Dirección de Planeación Estratégica y Sistemas de Información para garantizar la aplicación de las metodologías aquí desarrolladas.
- Cooperar con la Dirección de Planeación Estratégica y Sistemas de Información, cuando se requiera evaluar cómo el marco de apetito de riesgo ha sido incorporado en la gestión de sus procesos.
- El líder del proceso deberá asegurarse de que los terceros contratados realicen gestión sobre los riesgos y/o controles trasferidos y/o compartidos.
- Determinar el seguimiento a los controles establecidos para determinar su relevancia y actualizarlos de ser necesario.
- Verificar que los controles están diseñados e implementados de manera efectiva y operan como se pretende, para controlar los riesgos.

Todos los servidores son responsables de ejecutar los controles operativos en el día a día, como parte del desarrollo de sus funciones.

SEGUNDA LÍNEA DE DEFENSA – DIRECCIÓN DE PLANEACIÓN ESTRATÉGICA Y SISTEMAS DE INFORMACIÓN:

- Capacita, acompaña, genera recomendaciones y define la metodología.
- Generar propuestas sobre la Política para la Administración del Riesgo de la Entidad (metodología de gestión) y presentarlas para aprobación del Comité Institucional de Coordinación de Control Interno.
- Coordinar, liderar, capacitar y acompañar 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.
- Crear en el aplicativo los riesgos aprobados por el Comité Institucional de Gestión y Desempeño.
- Recomendar un marco de apetito de riesgo adecuado para CISA, consistente con los objetivos estratégicos y el modelo de negocio y presentar a las instancias correspondientes, cada vez que corresponda.
- Presentar al Comité Institucional de Gestión y Desempeño 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.
- 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.

Oficial de Seguridad de la información:

- Definir el procedimiento para la Identificación y Valoración de Activos de información.
- 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 para mejorar la eficiencia y eficacia de los 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.

Jefatura de Procesos y Productividad:

- Asesorar y acompañar a la primera línea de defensa que haga parte de los procesos críticos para la continuidad del negocio, en la realización de la gestión de riesgos asociados a los eventos de interrupción del negocio y en la recomendación para mejorar la eficiencia y eficacia de los controles para mitigar estos riesgos.

- Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos, asociados a la continuidad del negocio.

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 los riesgos de CISA.
- Verificar que los controles están diseñados e implementados de manera efectiva y de forma efectiva para mitigar los riesgos.
- Reportar sobre la posibilidad de riesgo de corrupción u otras denuncias en los procesos auditados de acuerdo con lo dispuesto en el Memorando Circular No. 046.
- 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.
- Realizar seguimiento a los riesgos consolidados en los Mapas de Riesgos de conformidad con el Plan Anual de Auditoría y reportar los resultados al Comité de Coordinación de Control Interno.
- Recomendar mejoras a la Política de Administración del Riesgo.
- Identificar y evaluar cambios que podrían tener impacto significativo en el Sistema de Control Interno que se identifiquen durante evaluaciones periódicas de riesgos y en los trabajos de auditoría interna.
- Revisar los cambios en el direccionamiento estratégico o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables.
- Promover ejercicios de autocontrol para que cada proceso monitoree los niveles de eficiencia, eficacia y efectividad de los controles.
- Revisar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas.

6. 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:** Traslada el análisis de eventos y riesgos críticos.

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. MARCO CONCEPTUAL DEL APETITO DE RIESGO

Es un 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 de este es proporcionar un conjunto integrado de medidas que le permitan 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.

8.1 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 a los grupos de interés que se le debe comunicar dicho marco son: Alta dirección y Líderes de los procesos.

8.2 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 encontrarse en la zona “moderado” con “muy baja”. 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 alta”, “moderado con muy alta”, esto implica que a diferencia de lo anterior, se deberán ejecutar planes de tratamiento que permitan mitigar, compartir o eliminar el riesgo, basados en la ejecución de actividades de fortalecimiento o generación de nuevos controles para contrarrestar los impactos.

9. ESTABLECIMIENTO DEL CONTEXTO INSTITUCIONAL

Son las condiciones internas y externas, que pueden generar eventos de oportunidades o afectar negativamente el cumplimiento de la misión y objetivos del proceso y de la entidad. Definir el contexto institucional contribuye al autoconocimiento frente a la exposición al riesgo, porque permite identificar las situaciones generadoras de riesgos, para articular los objetivos frente a las características del entorno interno y externo, los cuales deberán ser considerados posteriormente en la gestión del riesgo.

Central de Inversiones S.A. CISA., tiene establecida una misión, visión, objetivos estratégicos y planeación institucional contenidas en la plataforma estratégica, así como también la definición del contexto la cual se determinó mediante la herramienta 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. Esta se realizará cada vez que sea actualizada la matriz DOFA como parte de la planeación estratégica de CISA, mediante un ejercicio ejecutado por los líderes de proceso

quienes garantizarán la participación de sus equipos de trabajo con el apoyo de la Dirección de Planeación Estratégica y Sistemas de Información.

9.1 Establecimiento del 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:

Factores de Riesgo	Clasificación	Componente DOFA – CISA
Talento Humano	**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 un participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.	Existe cierto riesgo de que la entidad sufra pérdidas causadas por corrupción.
	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.	
	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.	Existe cierto riesgo de que la entidad sufra pérdidas causadas porque no haya retroalimentación por parte de las instancias superiores, desconocimiento del inventario de activos, bajo reconocimiento, no haya formación constante, no exista entendimiento de que es CISA. Sin embargo, las buenas prácticas son compartidas con los servidores; los indicadores permiten tomar decisiones, existe experticia

Factores de Riesgo	Clasificación	Componente DOFA – CISA
		comercial y necesidad de ampliación de canales de atención.
Tecnología	**Fallas tecnológicas:** Errores en hardware, software, telecomunicaciones y/o interrupción de servicios básicos.	Existe cierto riesgo de que la Entidad sufra pérdidas causadas por sistemas de información no dinámicos, no amigables y que limitan las tareas.
Procesos	**Ejecución y administración de procesos**: Pérdidas derivadas de errores en la ejecución y administración de procesos.	Existe cierto riesgo de que la Entidad sufra pérdidas causadas por: • El cambio en los procesos que pueda generar errores en el cumplimiento de los procedimientos. • Que no existen backup en todos los cargos. • Que cuando se realicen análisis de las fuentes no sean óptimas, o confiables. • Desconocimiento de los procesos de CISA. • Reprocesos o cadenas de valor ineficientes. • Inoportuno e incorrecto suministro de información por parte de otras áreas que no permitan los procesos más ágiles. • Tramites internos ineficientes.

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

9.2 Establecimiento del contexto externo

Es el ambiente externo en el cual CISA, busca alcanzar sus objetivos. Entenderlo es importante para garantizar que se tomen en consideración las partes interesadas externas, 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	Componente DOFA – CISA
		Daños a activos fijos/ eventos externos: Pérdida por daños o extravíos de los activos fijos por desastres

Factores de Riesgo	Clasificación	Componente DOFA – CISA
Eventos externos	Otros eventos externos: Pérdida derivada de otros eventos externos diferentes a los relacionados con fraude externo o infraestructura.	naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.
		Fraude externo: Pérdida derivada de actos de fraude por personas ajenas a la entidad (no participa personal de la entidad).
		Otros eventos externos: Existe cierto riesgo de que la entidad sufra pérdidas causadas por políticas externas, baja visualización, posicionamiento, tarifas y precios ofrecidos no atractivos frente al mercado.

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.

10. CLASES DE RIESGOS ADMINISTRADOS

Durante esta etapa se realiza la clasificación del riesgo según sus características; en CISA se clasifican 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	Posibilidad de que una entidad incurra en pérdidas originadas por fuentes como errores humanos, fallas tecnológicas o procesos, infraestructura, o por factores externos.
Salud y seguridad en el trabajo	Combinación de la probabilidad de ocurrencia de un evento o exposición y la severidad de la lesión o enfermedad que se puede dar por ese evento o exposición.
Corrupción	Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
Continuidad del Negocio	Posibilidad de interrupción que pueda afectar la continuidad de las operaciones críticas de CISA, a través de la indisponibilidad de instalaciones, tecnología, personal y procesos.
Riesgo fiscal	Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

Clases de riesgo	Definición
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 efectos [4].
Riesgo de LA/FT-FPADM	Es la posibilidad de pérdida o daño que puede sufrir una entidad al ser utilizada para cometer los delitos de lavado de activos, financiación del terrorismo o de la proliferación de armas de destrucción masiva LA/FT-FPADM.
Prácticas anticompetitivas	Es la posibilidad de recibir sanciones por incumplimientos legales o regulatorios, sufrir pérdidas financieras o pérdidas de reputación por fallas de cumplimiento con las leyes aplicables sobre protección de la libre competencia.

11. METODOLOGÍA GENERAL PARA LA ADMINISTRACIÓN DE RIESGOS

En el documento anexo a esta política 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 Identificación de Riesgos (Mapa de Riesgos)" y la etapa de monitoreo / revisión se realizará a través del aplicativo, descrito en el anexo "Instructivo para el monitoreo de riesgos en el aplicativo".

11.1 IDENTIFICAR EL RIESGO

El líder del proceso deberá identificar y describir el riesgo, cuyo ejercicio debe ser participativo entre su equipo de trabajo y el con apoyo de la Dirección de Planeación Estratégica y Sistemas de Información, con el objetivo de realizar un análisis de las actividades estratégicas ejecutadas por el proceso, los atributos de calidad de los productos, es fundamental identificar un riesgo claro para el entendimiento de todos los actores involucrados, así como su alcance.

11.1.1 Describir la posible materialización del riesgo

Se hace necesario, que el líder del proceso y su equipo establezcan con claridad las posibles situaciones de cuándo se entenderá materializado el riesgo, evento(s) que interrumpen el cumplimiento del objetivo del proceso. Para ello se hará necesario que se realice una descripción detallada de (los) evento(s) que posiblemente pudiesen pasar, pero solo se registrarán los que tengan como consecuencias pérdidas cuantificables y cualificables. En adelante se entenderá como la materialización objetiva del riesgo.

Para los riesgos de corrupción la descripción es la siguiente: "Materialización objetiva del riesgo: Una vez emitido el resultado final de la investigación en contra del servidor o exfuncionario respectivo por parte de la instancia correspondiente (contraloría, procuraduría, fiscalía, servidores internos competentes de realizar

[4] ISO/IEC 27000

la investigación etc.) que determine la existencia de un acto de corrupción dentro de CISA relacionado con el riesgo presente, se podrá establecer la materialización".

Dentro del contexto de riesgo fiscal, el impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público (bienes, intereses o recursos públicos), a la cual se vería expuesta CISA en caso de materializarse el riesgo.

Con respecto a los riesgos asociados a la continuidad del negocio, la materialización objetiva del riesgo se entenderá cuando se presente un evento de interrupción de la operación de los procesos críticos y no se cumplan los tiempos objetivos de recuperación (RTO) definidos para cada uno de ellos.

11.2 ANALIZAR EL RIESGO

El líder del proceso deberá analizar el riesgo, cuyo ejercicio debe ser participativo entre su equipo de trabajo y con el apoyo de la Dirección de Planeación Estratégica y Sistemas de Información, para establecer la probabilidad de ocurrencia e impacto[10] de sus efectos, con el fin de obtener información cuantitativa y cualitativa que establezca el nivel de riesgo inherente (sin controles). 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, estableciendo el grado de exposición del riesgo. Para esto, se debe cruzar en el mapa de calor la probabilidad e impacto y ubicarlo en la zona correspondiente, obteniendo así el nivel de riesgo inherente.

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.

Respecto de los riesgos de corrupción en el mapa de calor en el análisis, se realizará teniendo en cuenta los niveles "moderado", "mayor" y "catastrófico", debido a que estos riesgos siempre serán significativos, en este orden de ideas, no aplican los niveles de impacto "insignificante" y "menor".

11.3 VALORAR EL RIESGO

El líder del proceso deberá valorar el riesgo, cuyo ejercicio debe ser participativo entre su equipo de trabajo y con el apoyo de la Dirección de Planeación Estratégica y Sistemas de Información, realizan la identificación, descripción, documentación y calificación de los controles relacionados con el riesgo previamente analizado, los cuales deben estar directamente relacionados con las causas y efectos identificadas, para de este modo modificarlo, obteniendo como resultado el riesgo residual.

10 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.

11.4 TRATAMIENTO - MANEJO DEL RIESGO

El líder del proceso deberá tratar el riesgo, cuyo ejercicio debe ser participativo entre su equipo de trabajo y con el apoyo de la Dirección de Planeación Estratégica y Sistemas de Información, validando el tratamiento que se debe dar al riesgo en caso de identificar falta de controles en los procesos, debilidades en los controles o materializaciones de los riesgos.

11.5 MONITOREAR Y REVISAR

El líder del proceso deberá monitorear el riesgo, cuyo ejercicio debe ser participativo entre su equipo de trabajo y con el apoyo de la Dirección de Planeación Estratégica y Sistemas de Información, deben verificar el continuo estado de los riesgos operativos, de continuidad del negocio y de corrupción con el fin de identificar cambios a 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 25 del mes de abril, agosto y diciembre).

11.5.1 Materialización del Riesgo

Las causales de materialización de riesgos operativos, seguridad digital, fiscales, estratégicos, de LA/FT-FPADM, prácticas anticompetitivas y continuidad del negocio. La materialización del riesgo es uno de los temas de mayor impacto frente a la administración del riesgo, debido a que se hace referencia a la afectación comprobada que se presenta sobre los objetivos del proceso o producto tras la ocurrencia de un evento.
La materialización de un riesgo se debe reportar 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, toda vez que este genere una perdida reputacional y/o económica.

Para la acción de materializar un riesgo se debe tener en cuenta la descripción de la materialización objetiva definida en la identificación del riesgo; pero, si alguno de los motivos anteriormente relacionados llegase a presentarse, esto deberá ser causal inmediata para su materialización.

Cada vez que se materialice un riesgo se deberá actualizar el mapa de calor en el aplicativo correspondiente cambiando la probabilidad a la escala Muy Alta y dejando igual la escala del impacto. Se debe tener en cuenta que a medida que los controles sean efectivos en el tiempo, es decir el riesgo no se materialice, la probabilidad podrá disminuir paulatinamente en el riesgo residual hasta lograr el nivel más bajo. En este sentido, mientras la probabilidad no se ubique en la escala Muy Baja y los controles demuestren ser efectivos, el líder del proceso podrá solicitar a la Dirección de Planeación Estratégica y Sistemas de Información la actualización de la calificación del riesgo residual (aplica para los riesgos materializados).

11.5.2 Gestión de eventos

Un evento se puede considerar como los incidentes que generan pérdidas a CISA. Cada vez que se reporten eventos comprobados de esta naturaleza por parte de cualquier fuente, la Dirección de Planeación Estratégica y Sistemas de Información verificará que el líder del proceso haya realizado el registro correspondiente en el aplicativo, en caso de aplicar, para así obtener la base de eventos actualizada y con ello realizar el seguimiento respectivo.

11.5.3 Indicadores

Respecto del procedimiento el líder del proceso cuando haga registro de los indicadores del SIG formato perteneciente al manual 13 “Manual del SIG”. El indicador podrá estar asociado a un riesgo, en el seguimiento al cumplimiento del objetivo del proceso. Por tanto, se debe tener en cuenta que en caso de que el indicador no haya cumplido la meta, el líder del proceso deberá analizar y contestar las siguientes preguntas: ¿El resultado del indicador podría representar la posible materialización de un riesgo del proceso? ¿Los controles funcionan adecuadamente? En caso de responder sí, deberá reportar a la Dirección de Planeación Estratégica y Sistemas de la Información la posible materialización del riesgo de acuerdo con lo descrito en la presente política.

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

Todos los servidores 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.

13. ANEXOS

ANEXO No. 1	Metodología para la administración del riesgo en Central de Inversiones S.A.- CISA
ANEXO No. 2	Ficha Técnica Identificación de Riesgos (Mapa de Riesgos)
ANEXO No. 3	Metodología para la Gestión de Riesgos de Seguridad de la información e Informática
ANEXO No. 4	Plan de Tratamiento al Riesgo
ANEXO No. 5	Instructivo para el Monitoreo de Riesgos en el Aplicativo
ANEXO No. 6	Instructivo para la Gestión de Riesgos Estratégicos
ANEXO No. 7	Instructivo para la gestión de riesgos de salud y seguridad en el trabajo
ANEXO No. 8	Formato matriz de peligros y riesgos SST

14. 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””

Versión	Fecha	Motivo de la Revisión	Modificaciones
			Se modificó el numeral 5.1 “Difusión y Socialización de los mapas y planes de tratamiento del riesgo” el cual se llama ahora “Difusión y socialización del mapa de riesgo”. Se eliminó el numeral 5.3 “Manejo de Riesgos (Numeral 10.1.5 “Código de Buen Gobierno”). Igualmente se modificó la numeración de los numerales seguidos a este numeral. Se modificaron los numerales 5.3.1 “Procedimiento General”, 5.3.2 “Estructura del proceso de Administración del Riesgo”, 5.3.2.1 “Establecer el contexto estratégico”, 5.3.2.1 “Análisis del Riesgo”, 5.3.2.4 “Valoración del Riesgo”, 5.3.2.5 “Políticas de Administración del Riesgo”, 5.3.2.6 “Mapa de Riesgo”, 5.3.2.7 “Monitoreo del Riesgo y Tratamiento del Riesgo Residual” Se modificó el numeral 6.1 “Procedimiento para la Administración del Riesgo en CISA”
06	Mayo 11 de 2012	Implementación NTC ISO 31000:2009	Se modificó todos los numerales de la Circular Normativa por la implementación de la metodología para la Gestión del Riesgo sugerida por la norma NTC ISO 31000:2009. Se eliminó el anexo No. 1 “Guía para la Administración del DAFP” Se crearon los anexos No. 1 “Evaluación de la eficacia del Control”, No. 2 “Evaluación de la eficiencia del Control”, No. 3 “Mapa de Probabilidad de Ocurrencia”, No. 4 “Mapa de consecuencias, positivas o negativas” y No. 5 “Mapa 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

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

Versión	Fecha	Motivo de la Revisión	Modificaciones
			"Análisis de riesgos de corrupción", 5.5.1 "Valoración de riesgos operativos", 5.5.5 "Valoración de riesgos de corrupción" y 5.7 "Difusión y socialización del mapa de riesgo" Se eliminaron los numerales 5.1 "Difusión y socialización del mapa de riesgo", 5.2 "Desarrollo del criterio para la evaluación del riesgo, 5.3 "metodología", 5.3.1 "Procedimiento General", 5.3.2 "Estructura para la gestión del riesgo" y 5.3.2.1 "Diseño del marco de referencia para la gestión del riesgo". Se eliminaron los anexos No. 1 "Evaluación de la eficacia del Control", No. 2 "Evaluación de la eficiencia del Control", No. 3 "Mapa de Probabilidad de Ocurrencia", No. 4 "Mapa de consecuencias, positivas o negativas" y No. 5 "Mapa 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

Versión	Fecha	Motivo de la Revisión	Modificaciones
			del riesgo de corrupción", 5.2.6.3 "Niveles para calificar el riesgo de corrupción", 5.2.7.1 "Niveles para calificar el riesgo operativo", 5.2.7.2 "Nivel de aceptación del riesgo operativo", 5.2.9 "Periodicidad para el seguimiento de acuerdo al nivel de riesgo residual", 5.2.10 "Niveles de responsabilidad sobre el seguimiento y evaluación de riesgos". Se eliminaron los numerales 5.2 "Estrategia para la administración del riesgo", 5.3 "Lineamientos para el tratamiento de los 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	Se modificaron los numerales 3 "Alcance", 4 "Responsables", 6 "Normatividad Legal Aplicable",

Versión	Fecha	Motivo de la Revisión	Modificaciones
		riesgos de continuidad del Negocio.	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”. 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 Dirección de Planeación Estratégica y sistemas de información y Proyectos por la Dirección de Planeación Estratégica y sistemas de información, 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.

Versión	Fecha	Motivo de la Revisión	Modificaciones
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). Se modificó el anexo No. 1 "Ficha técnica para el levantamiento de riesgos (Mapa 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".
25	Diciembre 27 de 2021	Actualización del documento.	Se actualizo anexo No.1 y su denominación de" Ficha Técnica para el Levantamiento de Riesgos (Mapa de Riesgos)" a "Ficha Técnica Identificación de Riesgos Nuevos" Se actualizo las tablas de los numerales 11.1.2" Clasificar el Riesgo", 11.2.1.1.1 "Tabla de Clasificación de la Probabilidad: Escenario 1", 11.2.1.2.1" Tabla de Clasificación de la Probabilidad: Escenario 2", 11.3.2.3 "Medir el Riesgo Residual", 14 "Procedimiento para la Generación, Actualización y Seguimiento a la Gestión de Riesgo. Se reemplazo en todo el cuerpo de la circular normativa el nombre de "Eventos Naturales" a "Eventos Externos"

Versión	Fecha	Motivo de la Revisión	Modificaciones
26	Febrero 28 de 2022	Actualización de documentos.	Se actualizaron los numerales 4. “Responsables”, 9. “Marco Conceptual del Apetito del Riesgo” y 11. “Estructura para la Administración de Riesgos”.
27	Julio 21 de 2022	Actualización del documento, conforme lo aprobado por Comité Institucional de Coordinación de Control Interno realizado el 22/06/2022	Se actualizaron los anexos No. 1 “Ficha Técnica Identificación de Riesgos” y No. 3 “Plan de Tratamiento al Riesgo”. Se ajustaron los numerales No. 4. “Responsables”, 6. “Términos y Definiciones”, 9. “Marco conceptual del apetito de riesgo”, 10. “Establecimiento del contexto institucional” y 11. “Estructura para la administración de riesgos”.
28	Diciembre 1 de 2022	Actualización documento	Se ajustó la denominación de los cargos, conforme la estructura organizacional aprobada por Junta Directiva del 28/10/2022.
29	Enero 31 de 2023	Actualización del documento y Anexo	Se modificaron los siguientes numerales 1. “Política de Administración de Riesgos”, 2. “Objetivo”, 3. “Alcance”, 4. “Responsables”, 11.2.1.1.1 “Tabla de clasificación de la probabilidad: Escenario 1 riesgo operativo, corrupción, “, estratégico y continuidad del negocio, 11.2.1.2.1 “Tabla de clasificación de la probabilidad: Escenario 2 riesgo operativo, corrupción, estratégico, continuidad del negocio y seguridad digital” y 11.2.2.1 “Tabla de clasificación del impacto riesgo operativo, corrupción, estratégico, continuidad del negocio y seguridad digital”. Se actualizó el Anexo No. 2 “Instructivo para la Gestión de Riesgos de Seguridad Digital”.
30	Mayo 30 de 2023	Aprobación del Comité Institucional de Coordinación de Control Interno - 1ra Sesión Ordinaria (Presencial)el día 17 de mayo de 2023 08:30 a. m.-10:00 a. m.	Se actualiza numerales los numerales 1. “Política de administración de riesgos”, 2. “Objetivo” 3. “Alcance”, 5. “responsables”, 11.1 “Establecimiento del contexto interno”, 11.2 “Establecimiento del contexto externo”, 12. “Estructura para la administración de riesgos, 12.1. “Identificar el riesgo”, 12.1.4 “Describir la posible materialización del riesgo”, 12.1.5. “Identificar los factores del riesgo y clasificación del

Versión	Fecha	Motivo de la Revisión	Modificaciones
			riesgo".12.2.2.1. "Tabla de clasificación del impacto riesgo operativo, corrupción, continuidad del negocio y seguridad digital", 12.3.1. "Identificar controles", 12.3.1.1. "Tipos de controles", 12.3.2. "Diseño de los Controles para los riesgos operativos, corrupción y continuidad del negocio", 12.3.2.1. "Evaluar los controles individualmente", 12.5. "Monitorear y revisar", 13. "Mapa de riesgos", y numeral 15. "Procedimiento para la generación, actualización y seguimiento a la gestión de riesgo". Se crea el numeral 4. "Alineación Estratégica", y 12.2.1.2.2. "Tabla de clasificación de la probabilidad: Sin Escenario riesgo de continuidad del negocio. Se actualizó Anexos No.1 "Ficha Técnica Identificación de Riesgos", y Anexo No 4. "Instructivo para el Monitoreo de Riesgos en el Aplicativo de Seguimiento a la Estrategia – ASE"; Se creó el Anexo No 5. "Instructivo para la Gestión de Riesgos Estratégicos".
31	Diciembre 27 de 2023	Alineación metodología de identificación de peligros y riesgos de SST con la gestión del riesgo de CISA.	Se modificó el numeral 3 "Alcance". Se incluyeron los anexos No. 6 "Instructivo para la gestión de riesgos de salud y seguridad en el trabajo" y 7 "Formato matriz de peligros y riesgos SST"
32	Julio 19 de 2024	Actualización del documento de acuerdo con el comité institucional de Coordinación de Control Interno Acta N° 1 del 28 de Junio del 2024	Se modificaron los numerales 1" Declaración de la Política de Administración de Riesgos", 2" Objetivo", 3 "Alcance, 5" Responsables", 9. "Establecimiento del contexto Institucional", 9.2" Establecimiento del contexto externo" y todo el numeral 11" Metodología General para la Administración de Riesgos". Se creó el numeral 10 "Clases de Riesgos Administrados" Se eliminó el Anexo No. 2 "Instructivo para la Gestión de Riesgos de Seguridad Digital"

Versión	Fecha	Motivo de la Revisión	Modificaciones
			Se crearon los Anexos No 1 “Metodología para la administración del riesgo en Central de Inversiones S.A.- CISA” y No. 3 “Metodología para la Gestión de Riesgos de Seguridad de la información e Informática”. Se cambio la imagen corporativa de los Anexos No 5” Instructivo para el Monitoreo de Riesgos en el Aplicativo de Seguimiento a la Estrategia – ASE” y No 6” Instructivo para la Gestión de Riesgos Estratégicos”
32	Diciembre 03 de 2024	Actualización anexo	Se actualizó el Anexo No. 3 “Metodología para la Gestión de Riesgos de Seguridad de la información e Informática”.