Agencia Nacional
de Contratación Pública
Colombia Compra Eficiente

MANUAL METODOLÓGICO DEL SISTEMA DE ADMINISTRACIÓN DE RIESGOS

AGENCIA NACIONAL DE CONTRATACIÓN PÚBLICA

-COLOMBIA COMPRA EFICIENTE-

CONTENIDO

TABLA DE ILUSTRACIONES

TABLA DE TABLAS

I. INTRODUCCIÓN

La Agencia Nacional de Contratación Pública - Colombia Compra Eficiente (ANCP-CCE) define su Sistema de Administración de Riesgos (SAR) tomando como marco de referencia los lineamientos establecidos en la Guía para la Administración del riesgo del DAFP v6, el Modelo Estándar de Control Interno – MECI, y las directrices que establece el Estatuto Anticorrupción - Ley 1474 de 2011, la Ley de Transparencia y del Derecho de Acceso a la Información Pública - Ley 1712 de 2014, y los modelos internacionales implementados, que permiten fortalecer los mecanismos para la identificación, análisis, evaluación, tratamiento y monitoreo los riesgos que puedan afectar el logro de los objetivos institucionales; lo anterior en concordancia con lo expuesto por la Agencia en la Resolución 103 de 2013.

II. OBJETIVO GENERAL

Establecer los lineamientos para la adecuada gestión de riesgos de la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente (ANCP-CCE), a través de una metodología que permita de manera integral, eficaz, eficiente y efectiva, la identificación, análisis, evaluación, tratamiento, monitoreo, revisión, comunicación y consulta de los riesgos que pueden afectar el cumplimiento los objetivos estratégicos y de proceso, orientando la entidad hacia un nivel de aseguramiento razonable y una estructura de prevención y gestión de riesgos en la cadena de valor.

III. ALCANCE

Este manual debe ser aplicado por la línea estratégica y por las tres líneas de defensa teniendo en cuenta los roles y responsabilidades definidos para el Sistema de Administración del Riesgo SAR en la política del Sistema de Administración de Riesgos de la ANCP-CCE.

Así mismo, aplica para todas las tipologías de los riesgos e integra los asociados a los modelos internacionales que se implementen en la entidad (Seguridad y Salud en el Trabajo, Gestión Ambiental, Seguridad y Privacidad de la Información, Continuidad de Negocio), los riesgos fiscales, de fraude y corrupción. La presente metodología se aplica a través de la Suite Vision Empresarial.

IV. TÉRMINOS Y DEFINICIONES

∴ **Administración 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. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando

que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación. La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

- **Activo de información**: en el contexto de seguridad de la información son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- **Amenaza:** causa potencial de un incidente no deseado que puede resultar en perjuicio de un sistema o la organización.
- **Apetito de 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.
- **Autocontrol:** capacidad que tiene cada servidor público para detectar las desviaciones en su trabajo y realizar los correctivos necesarios; en tal virtud, la autoevaluación, como herramienta complementaria al autocontrol se convierte en un instrumento básico para la mejora continua de las entidades.
- **Autoevaluación:** comprende el monitoreo que se le debe realizar a la operación de la entidad a través de la medición de los resultados generados en cada proceso, procedimiento, proyecto, plan y/o programa, teniendo en cuenta los indicadores de gestión, el manejo de los riesgos, los planes de mejoramiento, entre otros.
- **Bien Público:** son todos aquellos muebles e inmuebles de propiedad pública.
- **Bien de uso público:** son todos aquellos muebles e inmuebles de propiedad pública. (Las calles, plazas, puentes, vías, parques etc.)
- **Bienes fiscales:** aquellos que están destinados al cumplimiento de las funciones o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades. (Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.)
- **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.
- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Ciclo de vida del proyecto:** serie de fases que atraviesa un proyecto desde su inicio hasta su cierre.

- **Confidencialidad:** propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
- **Consecuencia:** los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y/o demás partes interesadas.
- **Contenedor de la información:** cualquier plataforma tecnológica o lugar físico que almacena, procesa, transmite un Activo de Información por cualquier periodo de tiempo o propósito.
- **Contexto externo:** ambiente externo en el cual la organización busca alcanzar sus objetivos.
- **Continuidad del negocio:** Capacidad de una organización para continuar la entrega de productos o servicios a niveles predefinidos y aceptables tras una interrupción.
- **Control:** medida que permite reducir o mitigar un riesgo.
- **Control preventivo:** está diseñado para evitar un evento no deseado en el momento en que se produce.
- **Control detectivo:** está diseñado para identificar un evento o resultado no previsto después de que se haya producido. Busca detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes.
- **Disponibilidad**: propiedad de ser accesible y utilizable a demanda por una entidad.
- **Dueño del proceso:** funcionario de Colombia Compra Eficiente responsable del adecuado cumplimento de las actividades que conforman un proceso, y que están encaminadas a satisfacer una demanda tanto interna como externa a Colombia Compra Eficiente.
- **Evento:** ocurrencia o cambio de un particular conjunto de circunstancias. Un evento puede tener una o más consecuencias, o puede tener diferentes causas; puede consistir en algo no ocurrido, y puede ser referido algunas veces como un "incidente" o "accidente".
- **Establecimiento del contexto:** definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo.
- **Factores de riesgo:** son las fuentes generadoras de riesgos.
- **Fuentes de riesgo externas:** son eventos asociados a la fuerza de la naturaleza u ocasionados por terceros, que escapan en cuanto a su causa y origen al control de la entidad.
- **Gestión del riesgo:** actividades coordinadas para dirigir y controlar una organización con respecto al riesgo

- **Identificación del riesgo:** etapa en la cual se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias.
- **Impacto:** consecuencia o efecto que puede ocasionar a la organización la materialización del riesgo.
- **Integridad:** propiedad de exactitud y completitud.
- **Intereses patrimoniales de naturaleza pública:** son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica. A diferencia del recurso público, los intereses patrimoniales de naturaleza pública son expectativas.
- **Líder o responsable del proceso:** persona con la responsabilidad y autoridad para gestionar un riesgo.
- **Matriz de riesgos:** representación final de la probabilidad e impacto de uno o más riesgos de un proceso, plan, proyecto o programa.
- **Nivel de riesgo/severidad:** 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 o severidad es la combinación entre Probabilidad y la Consecuencia.
- **Patrimonio público:** se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C340-07).
- **Parte involucrada:** persona u organización que puede afectar o verse afectada o percibirse a sí misma como afectada por una decisión o una actividad.
- **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.
- **Proceso**: grupo de actividades relacionadas de manera lógica que, cuando se llevan a cabo, utilizan los recursos de Colombia Compra Eficiente para lograr resultados definitivos o transformar elementos de entrada, a través de una serie de actividades, en un producto o servicio.
- **Propietario del activo (o de la información):** funcionario encargado de identificar y establecer el alcance y valor o criticidad de un Activo de Información, los requerimientos de seguridad de este y la comunicación de éstos a los custodios del Activo de Información.

- **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 ambiental:** son los riesgos que están relacionados con la responsabilidad y compromiso de la entidad hacia el cuidado del ambiente.
- **Riesgo de corrupción:** posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgo estratégico:** se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
- **Riesgos financieros:** se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.
- **Riesgo fiscal:** es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.
- **Riesgo de fraude:** consisten en la posible pérdida financiera, material o reputacional que derivan de acciones, fraudulentas por actores internos o externos de la entidad.
- **Riesgos de imagen:** están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución, considerando el cumplimiento de requisitos legales.
- **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. Este nivel se determina antes de controles.
- **Riesgo legal:** se refiere al incumplimiento de leyes, normativas y regulaciones de diferente tipo, que son emitidas por el Gobierno Nacional y por otras entidades.
- **Riesgo operativo:** derivados de la definición y ejecución de los procesos, la operación de los sistemas de información y herramientas de apoyo a la gestión, de la estructura de la entidad y de los mecanismos de comunicación y articulación entre dependencias.

- **Riesgo reputacional:** es aquel que está asociado a los cambios de percepción u opinión sobre la entidad, que tienen sus grupos de valor.
- **Riesgo residual:** el resultado de aplicar la efectividad de los controles al riesgo inherente.
- **Riesgo reputacional:** es aquel que está asociado a los cambios de percepción u opinión sobre una empresa que tienen sus grupos de interés.
- **Riesgos de tecnología:** Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.
- **Riesgo de seguridad y salud en el trabajo:** son los riesgos que están relacionados con el compromiso de la entidad de preservar la salud y seguridad de los funcionarios, contratistas y pasantes.
- **Riesgos de seguridad de la información:** 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. (ISO/IEC 27000).
- **Recursos públicos:** dineros comprometidos y ejecutados en ejercicio de la función pública.
- **Seguridad de la información:** preservación de la Confidencialidad, Integridad y Disponibilidad de la información, en adición también de otras propiedades como autenticación, autorización, registro de actividad, no repudio y confiabilidad pueden ser también consideradas.
- **Tolerancia al 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:** establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (riesgo inherente).
- **Vulnerabilidad:** representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

1. RESPONSABILIDAD EN LA GESTIÓN DEL RIESGO

Para realizar un análisis y valoración del riesgo que permita mitigar efectivamente los riesgos identificados, la entidad tiene en cuenta las siguientes responsabilidades:

Tabla 1 Responsabilidades según líneas de Defensa

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Estratégica	Alta Dirección Comité Institucional de Coordinación de Control Interno Comité Institucional de Gestión y Desempeño	• Establecer y aprobar la Política de administración del riesgo la cual incluye los niveles de responsabilidad y autoridad. • Definir y hacer seguimiento semestral a los niveles de aceptación de riesgos (apetito, tolerancia y capacidad del riesgo). • Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles • Analizar los eventos y los riesgos críticos • Realizar seguimiento y análisis semestral a la gestión de riesgos y aplicar mejoras. • Evaluar el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento de este.
Primera Línea de defensa	Director General Subdirectores Secretario General Líderes de procesos	• Identificar, valorar y hacer seguimiento a los riesgos que pueden afectar los procesos, programas, proyectos y planes a su cargo y actualizarlos cuando se requiera. • Diseñar, ejecutar y hacer seguimiento a los controles definidos para mitigar los riesgos identificados. • Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos. • Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. • Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos

		• Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles, esto a través de los Subcomités de Control Interno • Reportar a la segunda línea de defensa los riesgos materializados en los procesos, programas, proyectos, y/o planes a su cargo. • Revisar los tratamientos establecidos para cada uno de los riesgos, con el fin de que se implementen y sean eficaces frente a la exposición de riesgo identificado. • Reportar en la herramienta de revisión de análisis estratégico RAE, los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado. • Los líderes de Procesos, propietarios y responsables de Activos de Información son los encargados de realizar la gestión del Riesgo sobre dichos Activos de Información. El Oficial de Seguridad de la Información, o quien haga sus veces, debe promover y apoyar la ejecución de esta actividad.
Segunda Línea de defensa	Asesor Experto con funciones de Planeación	• Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo. • Consolidar el Mapa de riesgos institucional y presentarlo para análisis y seguimiento en las instancias correspondientes (CIGD y CICCI). • Presentar al Comité Institucional de Coordinación de Control Interno el Sistema de Administración de Riesgos que adelanta la Agencia. • Acompañar, orientar, entrenar y establecer con los líderes de procesos la identificación, análisis y valoración de los riesgos. • Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos.

		• Monitorear los riesgos y controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos. • Desarrollar procesos de capacitación en temas relacionados con la gestión de riesgos de la Agencia • Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos • Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles. • Las responsabilidades en el seguimiento como 2da línea de los riesgos de seguridad de la información serán llevados a cabo por el Oficial de Seguridad, o quien haga sus veces, conforme a la normatividad y documentación vigente del MSPI[1]
Tercera Línea de defensa	Asesor Experto con funciones de Control Interno	• Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo de la Agencia, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos • Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa • Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, incluyendo los riesgos de corrupción • Evaluar la eficacia de los controles para la mitigación de los riesgos que se han establecido por parte de la Primera Línea de Defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos. • Revisar el perfil de riesgo inherente y residual por cada proceso, así como el perfil consolidado, y pronunciarse sobre cualquier

[1] Modelo de Seguridad y Privacidad de la Información

		riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad no sea coherente con los resultados de las auditorías realizadas. • 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 CICCI

Fuente: Manual Operativo Esquema de líneas de defensa V3

2. METODOLOGÍA PARA LA ADMINISTRACIÓN Y GESTIÓN DE RIESGOS

La Administración del Riesgo de la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente- (ANCP-CCE), sigue las fases de identificación y valoración de los riesgos, teniendo como marco de referencia la Guía para la Administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública (DAFP), y especificaciones para la Gestión de Riesgos previstas en las normas ISO 31000:2018, ISO 27001:2023, ISO 14001:2015 e ISO 45001:2018.

Las fases para la gestión integral del riesgo de la Agencia son: Establecer el contexto, identificación, análisis, evaluación y tratamiento del riesgo y de manera transversal: comunicación y consulta y monitoreo y seguimiento de los riesgos. Estas fases se aplican en la a través de la herramienta establecida para tal fin.

Ilustración 1 Fases para la administración de riesgos

Fuente: Elaboración Grupo de Planeación ANCP-CCE

2.1. Establecimiento del Contexto

En esta fase se establecen los parámetros internos y externos que se van a considerar para la administración del riesgo en la Agencia, se establece el objetivo, el alcance, los roles y responsabilidades con base en la normativa vigente, el contexto identificado por la Agencia a partir de lo establecido en el proceso CCE-DES-CP-01 Direccionamiento estratégico, el MIPG y los modelos internacionales.

La definición o actualización de la política se debe realizar cada vigencia y debe incluir los siguientes criterios:

- El objetivo que se espera alcanzar a partir de la administración de los riesgos.
- El alcance de aplicación, teniendo en cuenta la plataforma estratégica, el modelo de operación por procesos, los modelos internacionales implementados, los recursos, las actividades que se desarrollan en la Agencia para el cumplimiento de sus funciones.
- La tipología de los riesgos que se van a abordar, teniendo en cuenta la normativa aplicable y los modelos internacionales implementados.
- La definición de las responsabilidades y lineamientos para tener en cuenta en cada una de las fases del riesgo establecidas por la ANCP-CCE.

La aprobación y revisión periódica de la política de riesgos se realiza por parte de la Línea Estratégica de Defensa, en el marco del Comité Institucional de Coordinación de Control Interno (CICCI).

2.2. Identificación de Riesgos

Esta fase permite conocer los riesgos que pueden afectar el logro de los objetivos o la gestión de la entidad según con la aplicación correspondiente. La identificación de riesgos consiste en generar una lista de los posibles eventos indeseados que pueden tener impacto en los objetivos estratégicos, proceso, producto, servicios, activo o actividad operativa al cual se le está documentando el riesgo. De igual manera, la identificación de riesgos se realiza a partir del análisis por parte de la primera línea de defensa (ver Tabla 1), basados en su experiencia, los registros, diagramas de flujo, lluvia de ideas, análisis de sistemas o análisis de escenarios.

Para adelantar una adecuada identificación de riesgos es necesario tener en cuenta el análisis de indicadores, los mapas de riesgos anteriores, los resultados de las auditorías internas y externas, los informes de seguimiento y evaluación a la gestión de los procesos y las dependencias, los informes de PQRSD y la retroalimentación de los grupos de valor, entre otros. Estas fuentes de información permiten evidenciar la materialización de riesgos, por tanto, es indispensable su análisis al momento de identificar posibles riesgos en los procesos. Lo anterior con el propósito de observar algún riesgo que se haya presentado con anterioridad, cuya evidencia se hubiese identificado en alguna de las fuentes mencionadas.

La identificación de riesgos es desarrollada mediante el análisis y diligenciamiento de la siguiente información en la Suite Vision Empresarial:

- **Clasificación del riesgo:** los riesgos de la ANCP-CCE se clasifican de la siguiente manera:

    - **Estratégicos:** hace relación a los riesgos de los objetivos e iniciativas estratégicas donde la línea estratégica identifica y clasifica los riesgos asociados a la toma de decisiones en el momento de estructurar la planificación de la entidad y que pueden afectar el cumplimiento de los objetivos estratégicos.

    - **Tácticos:** hace relación a los riesgos de los objetivos de los procesos y productos (bienes o servicios) generados por la Agencia para la gestión por parte de la primera línea.

- **Operativos:** hace relación a los riesgos asociados a activos de información (en función de tipo y criticidad de activo, según inventario de activos), infraestructura física y actividades.

- **Objetivo estratégico/proceso/producto/activo/actividad operativa:** en este campo se escribe el nombre o título del elemento objeto del análisis.
- **Objetivo específico/activo específico/aspecto ambiental/tipo de peligro:** este campo se diligencia, indicando el objetivo frente al cual se analiza el riesgo o una descripción del elemento objeto de análisis.
- **Descripción del Riesgo:** en este campo se describe el riesgo considerando las siguientes indicaciones:

  - Redactar de forma clara y concisa para expresar específicamente el evento indeseado que podría presentarse.
  - Considerar los eventos que pueden impedir, afectar, degradar o retrasar el logro de los objetivos o la gestión a nivel estratégico, táctico u operativo según el nivel de aplicación.
  - Tener en cuenta la descripción de los tipos de riesgos considerados en la Administración de Riesgos de la ANCP-CCE.
  - No incluir la causa ni el efecto en la redacción del riesgo, sólo la situación o evento indeseado.

- **Tipo de riesgo:** en esta columna se selecciona la opción que se adhiera a la siguiente tipología de riesgos.
  - **Riesgo estratégico:** están relacionados con la planificación, diseño y conceptualización de la Entidad por parte de la Dirección, en relación con su marco estratégico: misión, visión, cumplimiento de los objetivos estratégicos y la definición de políticas.
  - **Riesgo operativo:** derivados del funcionamiento de los sistemas de gestión institucional, la definición y ejecución de los procesos, herramientas de apoyo a la gestión, de la estructura de la entidad y de los mecanismos de comunicación y articulación entre dependencias.
  - **Riesgo de corrupción:** posibles hechos que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
  - **Riesgo legal:** se refiere al incumplimiento de leyes, normativas y regulaciones de diferente tipo, que son emitidas por el Gobierno Nacional y por otras entidades.

- **Riesgo reputacional:** se refiere a los cambios en la percepción u opinión sobre la entidad, que tienen sus grupos de valor.
- **Riesgo de fraude:** actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso 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 entidad, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
- **Riesgo fiscal:** se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública. En esta guía, el evento potencial es equivalente a la causa raíz.
- **Riesgo de tecnología:** están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.
- **Riesgo ambiental:** son los riesgos que están relacionados con la responsabilidad y compromiso de la entidad hacia el cuidado del ambiente
- **Riesgo de seguridad y salud en el trabajo:** son los riesgos que están relacionados con el compromiso de la entidad de preservar la salud y seguridad de los funcionarios, contratistas y pasantes.
- **Riesgo de seguridad y privacidad de la información:** son los riesgos asociados con la afectación a la confidencialidad, la integridad y la disponibilidad de información.
- **Riesgo de continuidad del negocio:** identificar las amenazas internas y externas, incluyendo concentraciones de riesgo, que pueden causar la interrupción o pérdida de las actividades críticas de la agencia, así como la probabilidad (o frecuencia) de que ocurra una amenaza.

- **Causas:** se enumeran los medios, circunstancias y/o agentes que generan el riesgo identificado o que propician su materialización. Estas causas pueden ser intrínsecas (internas) al ser atribuidas a personas, métodos, equipos, materiales e instalaciones, directamente involucradas en el proceso, es decir debilidades de la entidad, o extrínsecas (externas) cuando provienen del entorno en el que se desarrolla el proceso, es decir amenazas.

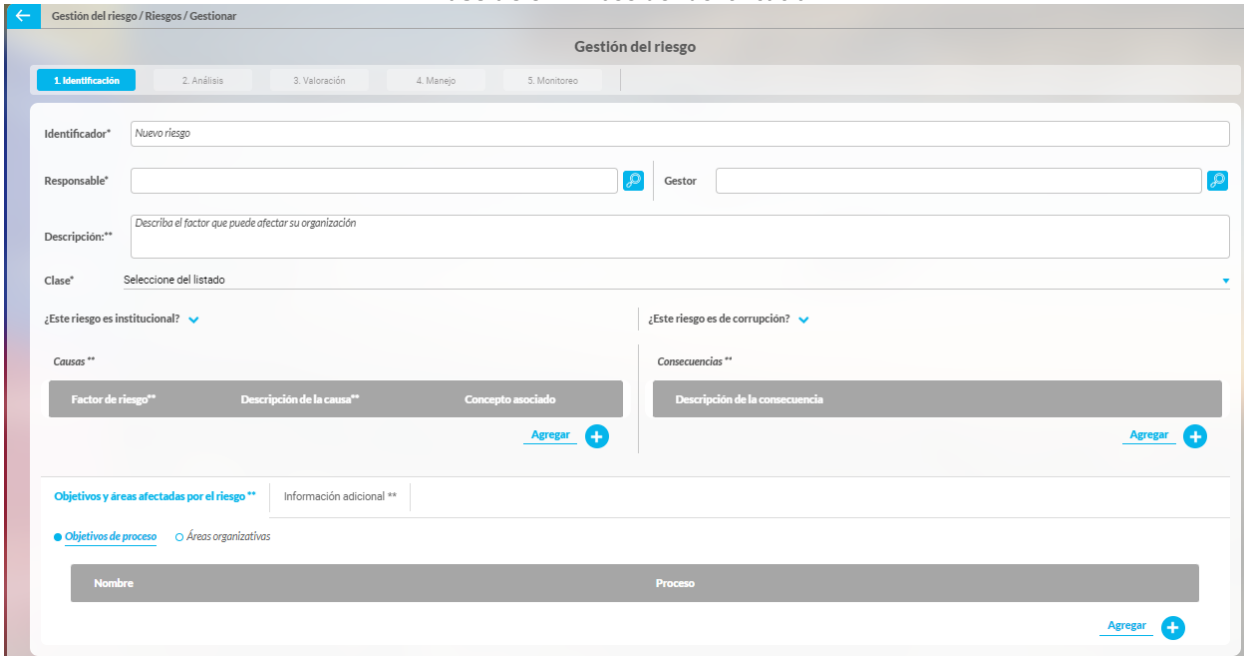
Con respecto a los riesgos de activos de información se pueden tener en cuenta los siguientes grupos causales:

- **Administración de información, software y hardware:** este grupo causal comprende todas las amenazas relacionadas con el correcto almacenamiento de la información y causas relacionadas directamente con fallas en el software y/o hardware.
- **Administración de usuarios y accesos:** este grupo causal comprende todas las amenazas relacionadas con el apropiado uso y administración de accesos a las diferentes áreas físicas, así como accesos a sistemas de información, aplicativos y cualquier sistema de información utilizado por la entidad.
- **Ataques maliciosos:** este grupo causal comprende todas las amenazas relacionadas con la corrupción de la información o los sistemas debido a un código malicioso.
- **Errores o causas humanas:** este grupo causal comprende todas las amenazas relacionadas con acciones que surgen del desconocimiento del flujo de información por parte de la persona que ejecuta el proceso.
- **Errores, fallas o ataques deliberados:** este grupo causal comprende todas las amenazas relacionadas con acciones que surgen de la intención de alterar, sustraer o manipular la información.
- **Infraestructura/edificios:** este grupo causal comprende todas las amenazas relacionadas con daños a las instalaciones o Hardware que puedan ser causados ya sea por desastres naturales (terremotos, inundaciones, etc.) por fallas en la infraestructura o falta de mantenimiento de esta.
- **Efectos/impactos:** hace relación a las consecuencias asociadas a la materialización del riesgo que inciden en el logro de objetivos, en la gestión de la entidad (operación, resultados, manejo de recursos) y/o afectaciones a partes interesadas. Los efectos no tienen relación uno a uno con las causas del riesgo, es decir, una o varias causas desencadenan el riesgo y la materialización de este ocasiona uno o varios efectos/impactos. Como ejemplos de efectos de riesgos se tienen:
    - Pérdidas económicas representadas en sobrecostos por reproceso, duplicidad o inactividad y detrimento del patrimonio, multas entre otras.
    - Detrimento de la imagen constituido por la pérdida de credibilidad y confianza en el cumplimiento de la misión y tareas encomendadas.
    - Sanciones legales constituidas por las sanciones que debe pagar la Entidad.
    - Afectación en la operación (misional y/o apoyo) de la entidad.
    - Consecuencias sobre la salud y seguridad de las personas que laboran en la Agencia.
    - Cambio en el medio ambiente, ya sea adverso o beneficioso, como resultado total o parcial de los aspectos ambientales de la entidad.

- **Proceso responsable del monitoreo del riesgo:** hace relación al proceso el cual realiza el seguimiento periódico al comportamiento del riesgo y al cumplimiento de las opciones de tratamiento que se definan.
- **Responsable del monitoreo:** hace relación al cargo o área responsable del objetivo, proceso, recurso o actividad sobre el que se monitorea el riesgo, quien debe hacer seguimiento a eventos de materialización y asegurar la definición y desarrollo de las opciones de tratamiento correspondientes, incluyendo su registro en la herramienta establecida para tal fin.

Lo anterior se debe diligenciar en el módulo de Gestión del riesgo / Riesgos / Gestionar: en la pestaña nuevo se despliega el siguiente cuestionario para la identificación:

Ilustración 2 Fase de Identificación



Fuente: Suite Vision Empresarial

2.3. Análisis del Riesgo

Posterior a la identificación, se realiza el análisis del riesgo puro o inherente donde se evalúan los riesgos sin considerar los controles que pudieran existir, analizando la naturaleza, las condiciones y la forma como se desarrolla la gestión en la entidad. Para ello, se determina la probabilidad de ocurrencia y el impacto de la materialización de cada riesgo identificado, en un escenario hipotético en donde los controles para prevenir o mitigar el riesgo no existen o no se aplican.

2.3.1 Análisis de probabilidad

Se establece la probabilidad de ocurrencia con la que se ha presentado o puede presentarse el riesgo antes de controles, seleccionando un nivel de probabilidad en una escala de muy baja, baja, moderada, alta y muy alta. Para seleccionar la calificación más adecuada se cuenta con varios criterios de análisis:

- **Descripción:** basada en una escala cualitativa para establecer el nivel de probabilidad de materialización del riesgo.
- **Frecuencia:** escala cuantitativa que se basa en él % de materialización del riesgo y por tanto aplica cuando se cuenta con medición de la ocurrencia de eventos de materialización, es decir datos históricos.
- **Frecuencia para actividades continuas:** escala cualitativa que presenta criterios de calificación de la probabilidad de materialización de eventos cuando las actividades que originan el riesgo son continuas.
- **Frecuencia para actividades o eventos ocasionales:** escala cuantitativa que presenta criterios para calificar la probabilidad de materialización de eventos cuando las actividades que originan el riesgo no son continuas ni frecuentes.
- **Frecuencia en función de la exposición:** esta escala ofrece criterios cualitativos para calificar la probabilidad de ocurrencia de un riesgo, asociándola con el nivel de exposición al peligro que lo genera; apoya especialmente, aunque no de forma exclusiva, el análisis de riesgos para la seguridad y salud en el trabajo.
- **Frecuencia en función de especialización requerida para que el riesgo ocurra:** escala cualitativa que aplica básicamente a riesgos de seguridad de la información, mediante criterios que indican el nivel de especialización necesario para explotar la vulnerabilidad que origina el riesgo.

Estos criterios se encuentran especificados en el Anexo 1 Criterios para el análisis de probabilidad.

2.3.2 Análisis de impacto

Establece la magnitud de los efectos ocasionados con la materialización del riesgo antes de controles, seleccionando un nivel de impacto en una escala de leve, menor, moderado, mayor, y catastrófico. Para realizar la calificación más adecuada se cuenta con los siguientes criterios establecidos:

- **Criterios transversales**
  - **Afectación en cumplimiento y resultados:** escala para calificación de impactos en el negocio, considerando la operación y los resultados de la gestión institucional.
  - **Afectación a grupos de valor:** escala para calificación de impactos que afectan de manera directa a los grupos de valor generando quejas, insatisfacción.
  - **Afectación reputacional o de imagen:** escala para calificación del impacto en la reputación, imagen y/o credibilidad de la dependencia y procesos.
  - **Afectación económica/fiscal:** escala para calificación del impacto económico o fiscal, en función de la afectación como sobrecostos, pérdidas financieras, variaciones de presupuesto, intereses, multas o sanciones pecuniarias.
  - **Afectación disciplinaria/legal:** escala para calificar el impacto disciplinario hasta las posibles implicaciones legales (penales o fiscales), sancionatorias, intervención de órganos de control.
- **Criterios específicos**
  - **Afectación SST:** escala para calificar el impacto en la salud y seguridad de los colaboradores en términos de lesiones, enfermedad e incapacidad.
  - **Impacto ambiental:** escala para calificar el impacto en función de la intensidad, extensión y reversibilidad de los aspectos ambientales. **Intensidad:** Grado de transformación que el impacto ambiental puede causar sobre el ambiente. **Extensión:** refleja la fracción del medio afectado respecto al entorno total **Reversibilidad:** capacidad del medio para recuperarse mediante mecanismos de autorregulación en el corto, mediano o largo plazo. El impacto es irreversible cuando el tiempo de permanencia a partir del cese de la actividad es superior a 15 años.
  - **Afectación en la seguridad de la información:** escala para calificar el impacto de los riesgos de seguridad de la información en función de la criticidad de los servicios, procesos, elementos o funciones afectadas por la disrupción, la cual se califica de manera consolidada a partir de la valoración de la propiedad del activo que haya sido afectado: confidencialidad, integridad y disponibilidad.
  - **Afectación en la continuidad del negocio:**
    - Escala para calificar el impacto en función de la criticidad de los servicios, procesos, elementos o funciones afectadas por la disrupción.

- Escala para calificar el impacto en función de del RTO contemplado para los servicios, procesos, elementos o funciones afectadas. RTO: Tiempo disponible para recuperar sistemas y/o recursos que han sufrido una alteración.

Estos criterios se encuentran especificados en el Anexo 2. Criterios para el análisis del impacto – criterios transversales y Anexo 3. Criterios para el análisis del impacto – criterios específicos.

Para el caso de riesgos de corrupción la estimación de consecuencia se determina a partir de la aplicación de la siguiente tabla:

Tabla 2 Criterios para definir el nivel de impacto en Riesgos de Corrupción

N.°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SÍ	NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de misión de la entidad?	X	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		X
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	X	
6	¿Generar pérdida de recursos económicos?	X	
7	¿Afectar la generación de los productos o la prestación de servicios?	X	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		X
9	¿Generar pérdida de información de la entidad?		X
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?	X	
11	¿Dar lugar a procesos sancionatorios?	X	
12	¿Dar lugar a procesos disciplinarios?	X	
13	¿Dar lugar a procesos fiscales?	X	
14	¿Dar lugar a procesos penales?		X
15	¿Generar pérdida de credibilidad del sector?		X
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		X
17	¿Afectar la imagen regional?		X
18	¿Afectar la imagen nacional?		X
19	¿Generar daño ambiental?		X
Responder afirmativamente de UNA a CINCO pregunta(s) genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.		10	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		
CATASTRÓFICO :	Genera consecuencias desastrosas para la entidad		

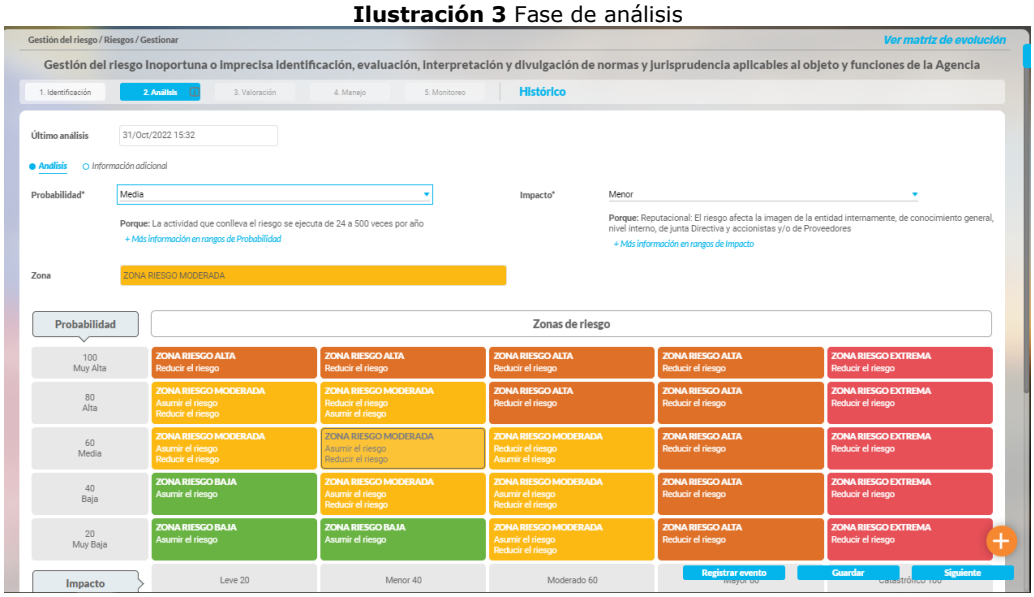
Nivel de impacto MAYOR

Fuente: Guía de administración de riesgos del Departamento Administrativos de la Función Pública

Lo anterior se debe diligenciar en el módulo de Gestión del riesgo/riesgos/gestionar:

Una vez guardada la información en la fase de identificación de despliega la información en la pestaña de análisis:

Ilustración 3 Fase de análisis

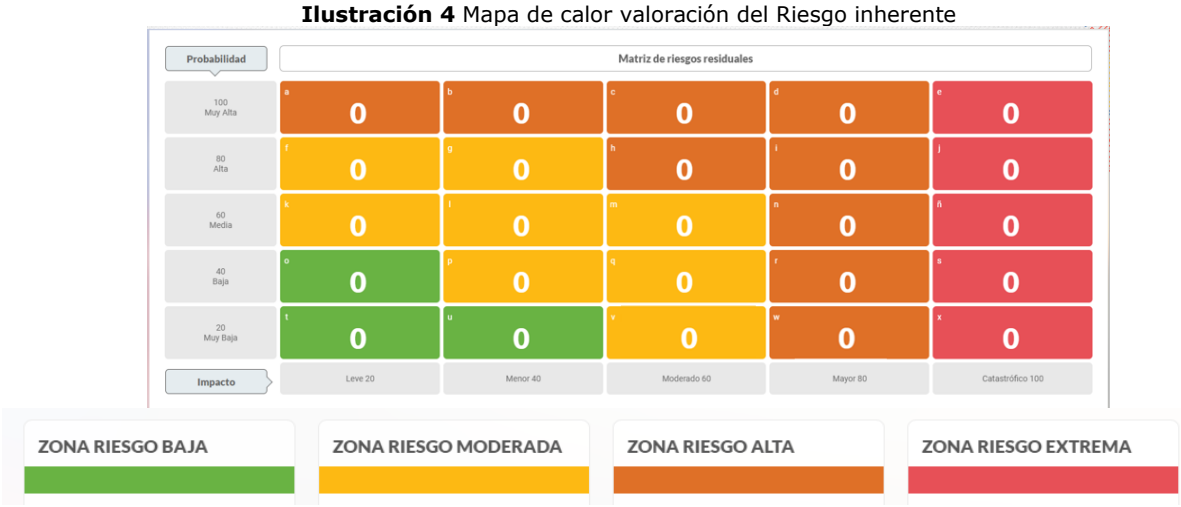


Fuente: Suite Vision Empresarial

2.3.3 Valoración del riesgo inherente

El nivel o zona de riesgo inherente se determina por la combinación de probabilidad y efecto/impacto, resultado que se ubica en alguna zona del mapa de calor. A continuación, se observa el Mapa de Riesgo que utilizará la Agencia en el desarrollo del Sistema de Administración de Riesgo.

Ilustración 4 Mapa de calor valoración del Riesgo inherente



Fuente: Suite Vision Empresarial

2.4. Evaluación del Riesgo

Para esta fase se identifican los controles existentes, se evalúan y califican según criterios que permiten determinar su robustez y a partir de ello se valora el riesgo residual.

Los criterios definidos para evaluación de los controles existentes en la Agencia son:

Tabla 3 Criterios para el diseño de controles

Descripción del control	Control se define como una medida de reduce o mitiga la causa generadora del riesgo.
Tipo de control	Hace referencia a la naturaleza y función del control. Los tipos de control son los siguientes: • Preventivos: son aquellas acciones encaminadas a eliminar las causas generadoras de un riesgo, de tal manera que eviten o disminuyan su ocurrencia o materialización. • Correctivos: son aquellas acciones que permiten el restablecimiento de la actividad, después de ser detectada la materialización del riesgo. • Detectivos: son aquellas acciones que permiten verificar o alertar sobre la posible materialización del riesgo. Para la eliminación de los peligros y la reducción o control de los riesgos para la Seguridad y Salud en el Trabajo, se utiliza la siguiente Jerarquización de los Controles:

	• EPP: uso de elementos de protección personal: Orientados a disminuir el impacto del peligro en la persona. •Administrativo: establecer políticas, procedimientos, prácticas del trabajo y programas de entrenamiento para reducir la exposición del riesgo. Pueden prevenir o detectar la presencia del riesgo. • Ingeniería: controles técnicos o de infraestructura que se aplican para aislar a las personas del peligro. Pueden ser preventivos o detectivos. • Sustitución: controles orientados a remplazar lo peligroso por una condición de menor grado de peligro. • Eliminación: controles orientados a eliminar el peligro.
Clase de control	Hace referencia a la manera en que se ejecuta el control: • Control automático: es aquel que funciona por sí solo, sin ayuda humana, generalmente está asociado a un sistema o tecnología informática. • Control semiautomático: ejerce su función a través de aplicativos o tecnología, pero requiere de la interacción humana para su funcionamiento. • Control manual: es aquel que se activa y funciona con acción humana.
Nivel de documentación del control	Esta información permite identificar si el control está documentado y si se conservan los soportes de su aplicación. Las opciones disponibles para seleccionar son: • Documentado y con soportes o evidencia de su aplicación. • Documentado, sin soportes de aplicación. • No documentado, con soportes de aplicación. • No documentado.
Definición de la responsabilidad del control	Se indica si la responsabilidad por la aplicación del control está asignada.
Frecuencia de aplicación del control	se selecciona de la lista desplegable la frecuencia con la cual es aplicado el control, las opciones son: • Permanente: cuando el control se aplica continuamente aun cuando la actividad que genera el riesgo no se esté ejecutando. • Periódica: cuando el control se aplica habitualmente bajo una frecuencia establecida (semanal, mensual, trimestral, semestral, anual, etc.).

	• Cada vez que se realiza la actividad: se selecciona cuando el control se activa con la ejecución de la actividad generadora del riesgo. • Aleatoria o no definida: cuando no se ha establecido una frecuencia para el control o no se ha aplicado regularmente o el control se aplica sobre una muestra seleccionada.
Eficacia del control en términos de su utilidad según el tipo de control	se valora si el control es útil siempre o algunas veces, para prevenir, corregir o detectar la materialización de un riesgo según el tipo de control seleccionado previamente.

Fuente: Elaboración Grupo de Planeación ANCP-CCE

2.5. Valoración del riesgo residual

Esta valoración utiliza la evaluación de los controles realizada en la fase de evaluación del riesgo, para determinar si con ellos se reduce la probabilidad de materialización del riesgo o el impacto que se calificó en la valoración del riesgo antes de controles (riesgo inherente), determinando así el riesgo no cubierto por los controles establecidos (riesgo residual). Este cálculo se realiza mediante la Suite Vision Empresarial.

Lo anterior se debe diligenciar en el módulo de Gestión del riesgo / Riesgos / Gestionar: Una vez guardada la información en la fase de análisis de despliega la información en la pestaña de valoración:

Ilustración 5 Fase de Valoración

Fuente: Suite Vision Empresarial

2.6. Tratamiento del Riesgo

Una vez realizado el análisis de riesgos y la evaluación de controles se establece el riesgo residual, para este se debe identificar la opción para su tratamiento teniendo en cuenta la siguiente tabla:

Tabla 4 Opciones de tratamiento de riesgos de acuerdo con la zona de riesgo

Zona de riesgo	Color	Opciones de tratamiento								
		Evitar o prevenir	Reducir - controles Administrativ	Reducir- controles de ingeniería	Reducir- uso de elementos de protección personal EPP	Reducir o mitigar	Compartir o transferir	Asumir	Compensar	Corregir
Extremo		X	X	X	X	X	X		X	X
Alto		X	X	X	X	X	X		X	X
Moderado		X	X	X	X	X	X	X	X	X
Bajo							X	X		

Fuente: Elaboración Grupo de Planeación ANCP-CCE

La opción seleccionada debe estar acorde con las necesidades y posibilidades de manejo. El tratamiento para el respectivo riesgo se registra en la Suite Vision Empresarial, según se explica a continuación:

- **Evitar o prevenir el riesgo:** tomar las medidas encaminadas para impedir la ejecución de la actividad que genera el riesgo / acciones encaminadas a evitar los impactos y efectos negativos que pueda generar la entidad sobre el ambiente.
- **Reducir o mitigar:** tomar las medidas que permitan mitigar o atenuar la probabilidad de materialización del riesgo, puede ser mediante acciones de naturaleza preventiva, correctiva o de mejora, fortalecimiento de controles existentes o la sustitución de un peligro por otro que no genere riesgo o que genere un riesgo de menor significancia / acciones dirigidas a minimizar los impactos negativos generados por la entidad sobre el medio ambiente.
- **Reducir el riesgo mediante controles administrativos:** tomar medidas encaminadas a disminuir la probabilidad de materialización del riesgo a través de decisiones administrativas que fortalezcan el proceso. En la gestión de riesgos de seguridad y salud en el trabajo, incluyen medidas que tienen como fin reducir el tiempo de exposición al peligro y acciones de señalización, advertencia, demarcación de zonas de riesgo, implementación de sistemas de alarma, diseño e implementación de procedimientos y trabajos seguros, controles de acceso a áreas de riesgo, permisos de trabajo, entre otros.
- **Reducir el riesgo mediante controles de ingeniería:** decisiones encaminadas a disminuir la probabilidad a través del rediseño de los procesos, así como las medidas técnicas para controlar peligros de seguridad y salud en el trabajo en su origen (fuente) o en el medio.
- **Reducir el riesgo mediante el uso de Elementos de Protección Personal (EPP):** tomar medidas basadas en el uso de dispositivos, accesorios y vestimentas con el fin de proteger las personas contra posibles daños a su salud o su integridad física derivados de la exposición a los peligros en el lugar de trabajo; estas medidas deben ser complementarias a los controles administrativos o de ingeniería.
- **Compartir o transferir el riesgo:** tomar medidas que reduzcan el efecto de la materialización del riesgo a través del traspaso de las pérdidas a otras organizaciones (externas e internas), como en el caso de los contratos de seguros, u otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido.
- **Asumir un riesgo:** cuando el riesgo es aceptable o tolerable puede quedar un riesgo residual que se decide mantener y en ese caso el Líder del Proceso acepta la pérdida residual. Si la materialización del riesgo que se decide asumir tiene un impacto moderado o de mayor significancia, el Líder del proceso debe definir las acciones o plan de contingencia que aplicará en caso de que el evento ocurra.

- **Compensar:** acciones dirigidas a resarcir y retribuir a la comunidad, región, localidad y al entorno natural por los impactos negativos generados por la entidad, que no puedan ser evitados, corregidos o mitigados.
- **Corregir:** acciones dirigidas a recuperar, restaurar o reparar las condiciones del ambiente afectado por la entidad.

2.7. Tratamiento del Riesgo

Una vez valorado el riesgo residual, se deben establecer los planes de tratamiento que contengan las acciones requeridas para cumplir con la opción de tratamiento seleccionada. Para los riesgos que queden en zona alta y extrema, en caso de que se considere necesario se pueden establecer planes de tratamiento para los riesgos que queden valorados en zona moderada y baja. concluidas las etapas de la administración de riesgos y se obtenga la valoración de los riesgos de gestión de la Entidad, se deben clasificar aquellos riesgos cuya calificación residual se encuentren en zonas Altas o Extremas. En estos casos, los procesos en los cuales se obtenga dicha calificación residual deberán formular un plan de tratamiento de riesgos que contenga las acciones requeridas para mitigar su ocurrencia e impacto dentro de la Agencia.

2.8. Registro de materialización de riesgos

En la ejecución de los procesos se pueden materializar riesgos para la entidad que deben ser reportados y manejados formalmente según lo descrito a continuación.

La identificación de eventos de materialización se puede dar en el desarrollo de los procesos, en la aplicación de los controles definidos o en la ejecución del monitoreo de riesgos.

Cuando un riesgo aplica a varias dependencias de la entidad, quien identifique un evento de materialización debe comunicar al responsable del monitoreo de dicho riesgo o al enlace de su dependencia, para que éste aplique el reporte y manejo según lo indicado a continuación.

Los eventos de materialización de riesgos deben ser registrados en la Suite Vision Empresarial por el responsable del monitoreo del riesgo, de modo que en el Grupo de Planeación consolide la información para el Monitoreo de Riesgos.

El reporte incluye indicar:

- **Fecha del evento de materialización:** día en el que ocurrencia del evento de materialización.
- **Descripción del riesgo:** se debe relacionar el riesgo materializado.

- **Situación de materialización:** se debe incluir la descripción de la situación en la que se presentó el evento de materialización.
- **Responsable que reporta el evento:** se debe relacionar el nombre, rol y la dependencia a la que pertenece la persona que realiza el reporte.
- **Acción de manejo del evento:** se debe relacionar las actividades que se ejecutaron para atender la materialización del riesgo.
- **Duración hasta la contención de la situación:** Tiempo de ejecución de las acciones tomadas**.**
- **Análisis de la materialización del riesgo:** a partir del análisis de la situación, se debe identificar la causa que generó el evento, los controles asociados a esta y las posibles modificaciones del riesgo en términos de probabilidad e impacto.
- **Recomendaciones de ajuste:** a partir del registro realizado por la dependencia, el grupo de planeación puede realizar recomendaciones sobre la identificación, análisis, evaluación o tratamiento del riesgo materializado.

Cuando la materialización de un riesgo modifica la calificación de probabilidad o impacto de manera que el nivel de riesgo residual no se mantiene (aumento en la probabilidad de ocurrencia o en el impacto del riesgo), es necesario formular un plan de mejoramiento

La materialización de los riesgos de Seguridad y Salud en el Trabajo se manejan teniendo en cuenta lo establecido por el Grupo de Talento Humano frente a el reporte, registro, investigación y análisis de accidentes e incidentes de trabajo y presuntas enfermedades laborales.

La gestión de incidentes de seguridad y privacidad de la información se realiza teniendo en cuenta lo establecido por el Grupo de Tecnología de la Información.

2.9. Monitoreo del Riesgo

El Monitoreo de Riesgos consiste en realizar una revisión y consolidación de la información reportada en la Suite Vision Empresarial, sobre el comportamiento de los riesgos, los eventos materializados, la aplicación y efectividad de los controles, el cumplimiento de los tratamientos, y posibles cambios en el contexto.

El monitoreo se realiza de manera mensual por parte de la segunda línea de defensa por medio del siguiente cuestionario que debe ser diligenciado por los enlaces de planeación designados en las dependencias:

1. Fecha de monitoreo
2. ¿Riesgo se materializo durante el periodo?
3. En caso afirmativo describa brevemente como se materializó, sus efectos y que acciones se tomaron para su mitigación y prevención
4. ¿El contexto sobre el cual existe la exposición del riesgo ha tenido algún cambio?
5. ¿Los controles se han aplicado sin novedad?
6. Validación de controles
7. Si el control no fue efectivo haga una breve explicación de porque fallo el control
8. Tiene alguna observación sobre el riesgo
9. Comentario de monitoreo
10. Fecha de próximo monitoreo

Nota: Las preguntas del cuestionario pueden variar teniendo en cuenta las necesidades del monitoreo de la gestión del riesgo de la Agencia.

Una vez consolidada y validada la información la segunda línea de defensa, se elabora el informe del monitoreo y mide el indicador *"Eficiencia del Sistema de Administración de Riesgos SAR"* el cual es aprobado por el Asesor(a) experto con funciones de planeación y socializado con la lideres de proceso.

De manera anual la segunda línea de defensa elabora un informe consolidado del Sistema de Administración del Riesgo a partir de la información reportada por la primera línea de defensa en los monitoreos mensuales.

2.10. Comunicación y Consulta

La segunda línea de defensa coordinara las acciones necesarias para promover la comunicación de información que promueva la cultura del Sistema de Administración del Riesgo ANCP -CCE- de manera integral de los riesgos gestionados por la entidad.

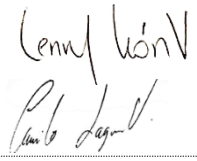
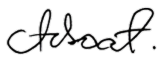
Se tiene establecida la herramienta Suite Vision Empresarial para la administra el sistema de riesgos y está disponible para consulta a través del siguiente usuario de consulta:

- Enlace: https://colombiacompra.pensemos.com/suiteve/base/client?soa=6& mnuId=suitevebaseclientsoa6soa6& clearpv=1&mis=headersve7-modules-menu-item-home
- Usuario: consulta
- Contraseña: 0000

De igual forma, la segunda línea de defensa determinará los mecanismos de divulgación, presentación y publicación de las matrices de riesgo y monitoreos de la Agencia, esto de acuerdo con las necesidades del público objetivo y/o los grupos de interés.

V. CONTROL DE CAMBIOS

FICHA TECNICA DE DOCUMENTO: 1. IDENTIFICACIÓN Y UBICACIÓN	
Título del documento:	MANUAL METODOLÓGICO DEL SISTEMA DE ADMINISTRACIÓN DE RIESGOS
Fecha de aprobación:	26/06/2024
Resumen / Objetivo de contenido:	Este documento establece los lineamientos para la gestión integral de riesgos de la Agencia Nacional de Contratación Pública – Colombia Compra eficiente, los cuales se aplican a través de lo establecido en las fases de identificación, análisis, evaluación, tratamiento, monitoreo y seguimiento y comunicación y consulta, con el fin de brindar un aseguramiento razonable de la Agencia para el cumplimiento de sus metas y objetivos institucionales.
Área / Dependencia de autoría:	Dirección General – Planeación
Código de estandarización:	CCE-DES-MA-02
Categoría / Tipo de documento:	Manual
Aprobación por:	Comité Institucional de Coordinación de Control Interno - CICCI
Información adicional:	N/A
Serie documental según TRD	DG.30.7 Manuales
Link de ubicación original del documento (especifique donde se aloja o reposa el documento)	https://www.colombiacompra.gov.co/transparencia/manuales

FICHA TECNICA DE DOCUMENTO: 2. AUTORES Y RESPONSABLES DE REVISIÓN Y APROBACIÓN				
Acción	**Nombre**	**Cargo/ Perfil**	**Fecha**	**Firma**
Elaboró	Lenny León Camilo Laguna	Contratistas	27/05/2024	
Revisó	Claudia Taboada	Asesora Experta con funciones de Planeación	17/06/2024	
Aprobó	Comité Institucional de Coordinación de Control Interno - CICCI	Comité Institucional de Coordinación de Control Interno - CICCI	21/06/2024	Acta Comité Institucional de Coordinación de Control Interno – CICCI 21/06/2024

Nota: Si la aprobación se realizó mediante acta de alguno de los comités internos considerados en la resolución número 173 de 2020 por favor especificar acta y mes del desarrollo de esta.

MANUAL METODOLÓGICO DEL SISTEMA DE ADMINISTRACIÓN DE RIESGOS

I. CONTROL DE CAMBIOS DE DOCUMENTO			Versión vigente del documento:		04
VERSIÓN	**FECHA**	**DESCRIPCIÓN DE AJUSTES**	**ELABORÓ**	**REVISÓ**	**APROBÓ**
01	23/10/2018	Creación del manual	Asesor Planeación Karina Blanco	Comité Directivo Resolución 1564 de 2018	Director General Juan David Duque
02	18/01/2019	Actualización vigencia 2019	Asesor Planeación Karina Blanco	Comité Directivo Resolución 1564 de 2018	Director General Juan David Duque
03	15/04/2020	Actualización vigencia 2020	Alirio Tovar Castellanos	Comité Institucional de Gestión y Desempeño	Comité Institucional de Coordinación de Control Interno
04	04/05/2021	Actualización vigencia 2021	Alirio Tovar Castellanos	Asesor Planeación Karina Blanco	Comité Institucional de Coordinación de Control Interno
05	20/06/2024	Actualización vigencia 2024	Lenny León	Asesora Planeación Claudia Taboada	Comité Institucional de Coordinación de Control Interno
Nota: El control de cambios en el documento, se refiere a cualquier ajuste que se efectúe sobre el documento que describe ficha técnica del presente documento.					

Anexo 1 Criterios de valoración de probabilidad

Nivel	Descriptor	Descripción	Frecuencia	Frecuencia para actividades continuas	Frecuencia para actividades o eventos ocasionales	Frecuencia en función de la exposición	Escala en función de especialización requerida para que el riesgo ocurra
1	**Muy baja**	La eventualidad de ocurrencia es muy baja, casi nula.	Ocurre ente el 0 – 19% de los casos	El evento ocurre anualmente	El evento nunca ha ocurrido	La situación de exposición se presenta de manera eventual durante la jornada laboral	Se requieren recursos o habilidades extremadamente especializadas para explotar la vulnerabilidad
2	**Baja**	El evento podría ocurrir sólo bajo circunstancias muy excepcionales.	Ocurre ente el 20 – 39% de los casos	El evento ocurre semestralmente	el evento ocurre una de cada 20 veces que se realiza la actividad	La situación de exposición se puede presentar alguna vez en un periodo de tiempo corto durante la jornada laboral	Se requieren recursos o habilidades de Administrador del Sistema o programador experimentado para explotar la vulnerabilidad
3	**Moderado**	El evento podría ocurrir en algún momento.	Ocurre ente el 40 – 59% de los casos	El evento ocurre mensualmente	el evento ocurre una de cada 10 veces que se realiza la actividad	La situación de exposición se puede presentar alguna vez por un periodo de tiempo prolongado durante la jornada laboral	Se requieren recursos o habilidades básicas de usuario TI y conocimientos generales del negocio para explotar la vulnerabilidad
4	**Alta**	El evento puede ocurrir algunas veces.	Ocurre entre el 60 – 79% de los casos	El evento ocurre semanalmente	el evento ocurre una de cada 5 veces que se realiza la actividad	La situación de exposición se puede presentar varias veces, por periodos de tiempo cortos durante la jornada laboral	Se requieren recursos o habilidades muy limitadas para explotar la vulnerabilidad
5	**Muy alta**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Ocurre entre el 80 – 100% de los casos	El evento ocurre diariamente	El evento ocurre una de cada dos veces que se realiza la actividad	La situación de exposición se puede presentar varias veces por periodos de tiempo prolongados durante la jornada laboral	No se requiere ningún recurso o habilidad especial. para explotar la vulnerabilidad

Anexo 2 Criterios para el análisis de impacto – Criterios transversales

Análisis del Impacto	Afectación en cumplimiento y resultados	Afectación a grupos de valor	Afectación Reputacional o de Imagen	Afectación Económica/ Fiscal	Afectación Disciplinaria / Legal
Descriptores del Impacto	**Escala para calificación de impactos en el negocio, considerando la operación y los resultados de la gestión institucional**	**Escala para calificación de impactos que afectan de manera directa a los grupos de valor generando quejas, insatisfacción**	**Escala para calificación del impacto en la reputación, imagen y/o credibilidad de la dependencia, procesos**	**Escala para calificación del impacto económico o fiscal, en función de la afectación como sobrecostos, pérdidas financieras, variaciones de presupuesto, intereses, multas o sanciones pecuniarias**	**Escala para calificar el impacto disciplinario hasta las posibles implicaciones legales (penales o fiscales), sancionatorias, intervención de órganos de control.**
1. Leve	Sin afectación en resultados Sin consecuencia en procesos ni actividades	No afecta a ningún grupo de valor de la entidad	Afecta la Imagen de la dependencia al interior de la entidad	No genera ningún costo adicional Genera pérdidas financieras insignificantes Genera variaciones de Hasta 0.5% del presupuesto de la entidad	Sin efectos disciplinario
2. Menor	Afecta resultados de la dependencia Incumplimientos que no generan reprocesos	Afectación parcial a algún grupo de valor, que no genera quejas	Genera pérdida de confianza, afectando su reputación a nivel interno	Genera Incremento de costos menos del 5% Genera variación Mayor o igual al 0.5% y menor al 5 % del presupuesto de la entidad	únicamente disciplinarias
3. Moderado	Afecta resultados del proceso Incumplimientos que generan reprocesos	Afectación a algún grupo de valor, generando quejas	Pérdida de Imagen, afectando su reputación a nivel Nacional	Genera Incremento de costos entre el 5% y 10% Genera variación mayor o igual al 5 % y menor al 10 % del presupuesto de la entidad	Disciplinarias, con posible intervención de órganos de control
4. Mayor	Afecta resultados en proyectos o Acciones estratégicas Afecta cumplimiento de plan de acción institucional.	Afectación a algún grupo de valor, disminuyendo niveles de satisfacción	Pérdida de confianza e imagen afectando su reputación a nivel Nacional	Genera incremento de costos entre el 10% y 20% Genera variación Mayor o igual al 10% y menor al 15 % del presupuesto de la entidad Genera pagos de intereses	Disciplinarias, con posible intervención de órganos de control y además efectos sancionatorios
5. Catastrófico	Afecta resultados en Objetivos Institucionales Afecta cumplimiento de indicadores PEI-Misión institucional	Afectación a varios grupos de valor	Afecta la Imagen de la entidad a nivel local, regional, nacional o Internacional	Incremento de costos más del 20% o variación mayor o igual al 15% del presupuesto de la entidad Genera indemnizaciones a terceros	Disciplinarias, con posibles efectos sancionatorios y además da lugar a procesos fiscales y/o penales

Anexo 3 Criterios para el análisis de impacto – Criterios específicos

Análisis del Impacto	Afectación SST	Impacto Ambiental	Afectación en la Seguridad de la Información	Afectación en la continuidad del negocio	
Descriptores del Impacto	**Escala para calificar el impacto en la salud y seguridad de los colaboradores en términos de lesiones, enfermedad e incapacidad**	**Escala para calificar el impacto en función de la intensidad, extensión y reversibilidad de los aspectos ambientales.** **Intensidad: G**rado de transformación que el impacto ambiental puede causar sobre el ambiente. E**xtensión:** refleja la fracción del medio afectado respecto al entorno total R**eversibilidad:** capacidad del medio para recuperarse mediante mecanismos de autorregulación en el corto, mediano o largo plazo. El impacto es irreversible cuando el tiempo de permanencia a partir del cese de la actividad es superior a 15 años.	**Escala para calificar el impacto de los riesgos de seguridad de la información en función de la criticidad de los servicios, procesos, elementos o funciones afectadas por la disrupción, la cual se califica de manera consolidada a partir de la valoración de la propiedad del activo que haya sido afectado: confidencialidad, integridad y disponibilidad.**	**Escala para calificar el impacto en función de la criticidad de los servicios, procesos, elementos o funciones afectadas por la disrupción.**	**Escala para calificar el impacto en función de del RTO contemplado para los servicios, procesos, elementos o funciones afectadas** **RTO: Tiempo disponible para recuperar sistemas y/o recursos que han sufrido una alteración.**
1. Leve	Lesiones o enfermedades que no requieren incapacidad.	Grado de transformación baja o mínima, extensión puntual con reversibilidad en el corto plazo	Todas las propiedades del activo afectado se puntúan o clasifican como "Información Pública" y "BAJA".	La interrupción tiene un impacto menor si no afecta ninguno de los servicios, procesos, elementos o funciones críticas y/o sensibles identificados en el BIA vigente.	Si la recuperación del servicio afectado puede ser igual o mayor de 24 horas.
2. Meno r	Lesiones o enfermedades con incapacidad menor a una semana.	Grado de transformación media, extensión parcial con reversibilidad en el mediano plazo.	Al menos una de las propiedades el activo afectado puntúa como "Información Pública Clasificada" o "MEDIA".	La interrupción tiene un impacto menor si afecta parcialmente alguno de los servicios, procesos, elementos o funciones críticas y/o sensibles identificados en el BIA vigente, pero dicha afectación sólo afecta servicios, procesos o funciones valorados con criticidad BAJA.	Si el RTO para los servicios, procesos, elementos o funciones críticas y/o sensibles afectados es de 12 a 24 horas.
3. Moderado	Lesiones o enfermedades con incapacidad entre una semana y 29 días	Grado de transformación alta, extensión extensa con reversibilidad en el largo plazo	Dos propiedades del activo afectado puntúan como "Información Pública Clasificada" o "MEDIA".	La interrupción tiene un impacto moderado si afecta parcialmente alguno de los servicios, procesos, elementos o funciones críticas y/o sensibles identificados en el BIA vigente, pero dicha afectación sólo	Si el RTO para los servicios, procesos, elementos o funciones críticas y/o sensibles afectados es de 8 a 12 horas.

				afecta servicios, procesos o funciones valorados con criticidad MEDIA.	
4. Mayor	Lesiones o enfermedades con incapacidad entre 30 días y 6 meses	Grado de transformación muy alta, extensión total con reversibilidad en el largo plazo	Dos propiedades del activo afectado están siendo afectadas: una (1) como "Información Pública Reservada" o "ALTA" y una como "Información Pública Clasificada" o "MEDIA".	La interrupción tiene un impacto mayor si afecta parcialmente alguno de los servicios, procesos, elementos o funciones críticas y/o sensibles identificados en el BIA vigente, pero dicha afectación sólo afecta servicios, procesos o funciones valorados con criticidad ALTA.	Si el RTO para los servicios, procesos, elementos o funciones críticas y/o sensibles afectados es de 4 a 8 horas.
5. Catastrófico	Lesiones o enfermedades graves o irreparables (con incapacidad permanente o invalidez)	Grado de transformación total, extensión crítica, irreversible	Dos o tres propiedades del activo afectado puntúan como "Información Pública Reservada" o "ALTA".	La interrupción tiene un impacto catastrófico si afecta totalmente alguno de los servicios, procesos, elementos o funciones críticas y/o sensibles identificados en el BIA vigente, pero dicha afectación sólo afecta servicios, procesos o funciones valorados con criticidad ALTA.	Si el RTO para los servicios, procesos, elementos o funciones críticas y/o sensibles afectados es de 0 a 4 horas.