Agencia Nacional
de Contratación Pública
Colombia Compra Eficiente

MANUAL METODOLOGICO PARA LA GESTIÓN INTEGRAL DE RIESGOS

AGENCIA NACIONAL DE CONTRATACIÓN PÚBLICA
-COLOMBIA COMPRA EFICIENTE-
2026

MANUAL METODOLOGICO PARA LA GESTIÓN INTEGRAL DE RIESGOS

CONTENIDO

TABLA DE ILUSTRACIONES

TABLA DE TABLAS

MANUAL METODOLOGICO PARA LA GESTIÓN INTEGRAL DE RIESGOS

1. INTRODUCCIÓN

La Agencia Nacional de Contratación Pública – Colombia Compra Eficiente (ANCP-CCE) identifica y gestiona de manera integral los riesgos, a partir de un sistema aplicable de manera transversal a la gestión institucional, que permita aplicar las fases y abordar aquellos eventos, vulnerabilidades, aspectos, peligros, actuaciones y situaciones tanto internas como externas, que puedan afectar o impedir el logro de los objetivos estratégicos.

La gestión de riesgos en la ANCP-CCE se fundamenta en los principios de la ISO 31000:2018, buenas prácticas internacionales basadas en el marco COSO ERM, la Guía para la Gestión Integral del Riesgo del DAFP (V7), el Modelo Integrado de Planeación y Gestión (MIPG) y el Modelo Estándar de Control Interno (MECI). El enfoque es transversal e integrado al SIG, permitiendo una administración articulada de los riesgos estratégicos, tácticos, operativos, tecnológicos, ambientales, de seguridad y salud en el trabajo, de seguridad de la información, de integridad pública (corrupción, fraude, soborno, conflicto de intereses, lavado de activos, financiación del terrorismo y proliferación de armas de destrucción masiva) y continuidad del negocio.

2. OBJETIVO GENERAL

Establecer los lineamientos metodológicos para la gestión integral de riesgos en la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente (ANCP-CCE), que permitan identificar, analizar, evaluar, tratar, monitorear y revisar los riesgos que puedan afectar el cumplimiento de los objetivos institucionales, la generación de valor público y el desempeño institucional.

3. ALCANCE

La metodología para la gestión integral de riesgos de la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente (ANCP-CCE) es de aplicación obligatoria para la línea estratégica y las tres líneas de defensa, en el marco de los roles y responsabilidades definidos en la política de riesgos.

La gestión de riesgos integra de manera transversal las diferentes tipologías de riesgo que pueden afectar el logro de los objetivos institucionales y la generación de valor público, en coherencia con los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG), la Guía para la Gestión Integral del Riesgo del Departamento Administrativo de la Función Pública y los modelos internacionales adoptados por la Entidad.

La aplicación de la metodología se realiza a través de las herramientas institucionales definidas para la gestión de riesgos, garantizando su integración con los procesos de planeación, seguimiento, evaluación, mejora continua y toma de decisiones.

El SIGRIP —Sistema de Gestión de Riesgos para la Integridad Pública— no es un componente separado, sino el marco integral bajo el cual se gestiona la totalidad de los riesgos institucionales, articulando la integridad pública de manera transversal en cada fase del ciclo de gestión.

4. 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: s**on 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 Defectivo:** 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.
- **Debida diligencia:** proceso de investigación y verificación aplicado a contrapartes (proveedores, contratistas, aliados, funcionarios en cargos de riesgo) para identificar señales de alerta relacionadas con riesgos de integridad, corrupción, LA/FT/FP u otros riesgos críticos.
- **Disponibilidad**: propiedad de ser accesible y utilizable a demanda por una entidad.
- **Líder 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:** circunstancia o condición que aumenta la probabilidad de que ocurra el evento de riesgo. No es la causa directa, pero incrementa el nivel de exposición.
- **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.
- **Función de Cumplimiento:** componente del SIGRIP que garantiza que la entidad identifique, gestione y mitigue los riesgos de incumplimiento legal, ético y de integridad. Incluye el responsable de cumplimiento, el canal de denuncias, los procedimientos de investigación y los mecanismos de reporte.
- **Gobernanza del Riesgo:** arreglos institucionales y de control que aseguran que los riesgos sean conocidos, comunicados, gestionados y monitoreados en toda la entidad, con liderazgo de la Alta Dirección.
- **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.
- **Indicador Clave de Riesgo (KRI – Key Risk Indicator):** métrica que proporciona información temprana sobre el aumento de la exposición al riesgo, permitiendo tomar acciones preventivas antes de que el riesgo se materialice. Diferente al KPI, que mide el desempeño del proceso ya alcanzado.
- **Integridad (seguridad de la Información):** propiedad de exactitud y completitud.
- **Integridad Pública:** alineación consistente de los valores, principios y acciones institucionales con los propósitos del servicio público, previniendo conductas que puedan afectar la confianza ciudadana y los recursos del Estado.
- **LA/FT/FP:** Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP).
- **Nivel de riesgo / Severidad:** valor que se determina a partir de combinar la probabilidad de ocurrencia y la magnitud del impacto del riesgo.
- **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 Riesgo:** 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:** posibilidad de que se generen impactos ambientales negativos o incumplimientos de requisitos ambientales derivados de las actividades de la entidad, afectando el desempeño ambiental institucional.
- **Riesgo de conflicto de interés:** Se presenta cuando el interés general, propio de la función pública, entre en conflicto con un interés particular y directo del servidor público. El interés del servidor público se presenta cuando debe decidir sobre asuntos en los que tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tiene su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho. (A partir de la Ley 1952 de 2019, art. 44, Ley 734 de 2002 y algunas disposiciones de la Ley 1474 de 2011).
- **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 emergente:** riesgo nuevo o en evolución, con alta incertidumbre y limitada información histórica, que puede identificarse en cualquier nivel de la gestión institucional
- **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:** Consiste en la posible pérdida financiera, material o reputacional que derivan de errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros. Puede ser interno, en cuyo caso el fraude involucra a colaboradores, o externo, cuando se realiza por terceros, externos y la organización es la víctima.
- **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 DE LA/FT:** La posibilidad de pérdida o daño que puede sufrir una entidad vigilada por su propensión a ser utilizada directamente o a través de sus operaciones como instrumento para el lavado de activos, canalización de recursos hacia la realización de actividades terroristas y/o financiación de armas de destrucción masiva, o cuando se pretenda el ocultamiento de activos provenientes de dichas actividades.
- **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 su 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:** combinación de la probabilidad de que ocurran uno o más eventos o exposiciones peligrosas en el desarrollo

de las actividades laborales, y la severidad de la lesión o enfermedad que pueden sufrir los funcionarios, contratistas y pasantes como consecuencia de estos. Decreto 1072 de 2015.

- **Riesgo 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).
- **Riesgo de soborno:** Oferta, promesa, entrega, aceptación o solicitud de una ventaja indebida de cualquier valor (que puede ser de naturaleza financiera o no financiera), directamente o indirectamente, e independientemente de su ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o deje de actuar en relación con el desempeño de las obligaciones de esa persona.
- **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.
- **SIGRIP:** Sistema de Gestión de Riesgos para la Integridad Pública, requerido por el Decreto 1122 de 2024. Comprende el conjunto de políticas, procesos, procedimientos y herramientas para identificar, prevenir, detectar y responder a los riesgos que puedan afectar la integridad pública y el ejercicio ético del servicio.
- **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.

5. CONTEXTUALIZACIÓN PARA LA GESTIÓN DEL RIESGO

La gestión de riesgos institucional se establece como un proceso integral y continuo que parte de la identificación y análisis del contexto interno y externo, con el propósito de asegurar la alineación de la entidad frente a los factores que pueden afectar el cumplimiento de sus objetivos estratégicos. Esta comprensión del contexto constituye la base para la formulación y actualización de la política de riesgos, así como para la definición de lineamientos que orienten su implementación en todos los niveles, integrando principios de gobierno, cultura y control interno. A partir de este marco, se habilita tanto el desarrollo de la política de gestión de riesgos como la estructuración de un modelo de medición del nivel de madurez, que permita evaluar de manera sistemática las capacidades institucionales, identificar oportunidades de

fortalecimiento y orientar la mejora continua conforme a las mejores prácticas internacionales.

6. POLÍTICA PARA LA GESTIÓN INTEGRAL DEL RIESGO

- **Objetivo de la Política (declaración y compromiso)**

La Agencia Nacional de Contratación Pública – Colombia Compra Eficiente (ANCP-CCE) Identifica y gestiona de manera integral los riesgos, a partir de un sistema aplicable de manera transversal a todo el modelo de operación de la agencia, que permita aplicar las fases y abordar aquellos eventos y vulnerabilidades, tanto internas como externas, que puedan afectar o impedir el logro de los objetivos estratégicos.

La gestión de riesgos en la ANCP-CCE se fundamenta en los principios de la ISO 31000:2018, buenas prácticas internacionales basadas en el marco COSO ERM, la Guía para la Gestión Integral del Riesgo del DAFP (V7), el Modelo Integrado de Planeación y Gestión (MIPG) y el Modelo Estándar de Control Interno (MECI). El enfoque es transversal e integrado al SIG, permitiendo una administración articulada de los riesgos estratégicos, tácticos, operativos, tecnológicos, ambientales, de seguridad y salud en el trabajo, de seguridad de la información, de integridad pública (corrupción, fraude, soborno, conflicto de intereses, lavado de activos, financiación del terrorismo y proliferación de armas de destrucción masiva) y continuidad del negocio.

La ANCP- CCE, como ente rector en materia de contratación pública, deberá actuar de forma ética, transparente y eficiente, en el marco del valor institucional de la honestidad, prohíbe cualquier práctica relacionada con actos, conductas y situaciones asociados a la corrupción, soborno, conflicto de intereses, el lavado de activos, financiación del terrorismo y proliferación de armas de destrucción masiva en cualquiera de sus formas, y promueve en todos sus colaboradores y grupos de valor, actuar de manera íntegra de acuerdo con el ordenamiento legal.

- **Alcance**

Aplica a todas las dependencias, productos y servicios, procesos, servidores(as) públicos de la entidad, grupos de valor y partes interesadas en todos los niveles jerárquicos y áreas estratégicas, misionales, de apoyo y evaluación. Incluye 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, Gestión Documental, Gestión del Conocimiento, los riesgos fiscales y de integridad pública, en el marco de la gestión institucional.

- **Responsabilidades**

Se establecen de acuerdo con la estructura de las líneas de defensa:

Línea estratégica de Defensa: Comité de Gestión y Desempeño Institucional y Comité Institucional de Control Interno.
1a línea de defensa: Responsables por Objetivos Institucionales, Líder del Proceso y/o responsables operacionales de los subsistemas del SIG.
2a línea de defensa: Grupo de Planeación, responsables operacionales de los componentes del SIG, líderes de políticas MIPG y responsable con función de cumplimiento.
3a línea de defensa: Asesora experta con funciones de Control Interno.

- **Fases para la Gestión del Riesgo**

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: **monitoreo** y seguimiento y, comunicación y consulta de los riesgos.

En cada una de las fases del ciclo de gestión del riesgo (contexto, identificación, análisis, evaluación y tratamiento), deben considerarse de manera transversal los escenarios de riesgo relacionados con integridad pública. Como controles estandarizados, la Agencia cuenta con un canal seguro, anónimo y accesible para recibir denuncias sobre hechos que puedan constituir riesgos de integridad pública, garantizando la confidencialidad y protección del denunciante. Así mismo, se implementan acciones de debida diligencia que permitan el conocimiento y evaluación de las contrapartes (proveedores, contratistas, aliados estratégicos), orientados a prevenir la vinculación con actividades que puedan ser utilizadas como vehículos para el LA/FT/FP. Estas fases se describen en el procedimiento, en el Manual Metodológico CCE-DES-MA-02 y se aplican en la SVE.

- **Criterios de Valoración, Apetito y Tratamiento**

Los riesgos se analizan considerando niveles de probabilidad e impacto, determinando el riesgo inherente y residual mediante la valoración de controles. El apetito se estructura en cuatro zonas (Extremo, Alto, Moderado, Bajo). Los niveles diferenciados por tipología son: tolerancia cero para riesgos de integridad pública (corrupción, fraude, soborno, LA/FT/FP) y SST graves — estos riesgos NUNCA se asumen, solo se evitan o previenen y siempre tienen impacto extremo; apetito bajo para riesgos fiscales, seguridad de la información y continuidad del negocio; apetito moderado para riesgos de gestión y operativos. Las opciones de tratamiento son: Evitar/Prevenir, Reducir/Mitigar, Compartir/Transferir, Asumir, Compensar y Corregir, conforme a la zona de riesgo definida en la metodología.

- **Niveles de riesgo y criterios de aceptación**

El apetito de riesgo se establece a partir de las cuatro (04) zonas del nivel de riesgo: extremo, alto, moderado y bajo, las cuales se distribuyen según el mapa de calor que combina los criterios de probabilidad e impacto. Se prioriza la definición e implementación de opciones de tratamiento para los riesgos que a nivel residual se valoren como alto y extremo.

En los casos en que se requiera se pueden establecer los planes de tratamiento para los riesgos que a nivel residual queden valorados en zonas moderada o baja.
Se debe tener en cuenta que los riesgos de integridad pública, en ningún caso serán "Asumidos".

- **Tratamiento**

Las opciones de tratamiento que aplican son: Evitar, prevenir, reducir o mitigar, compartir o transferir, asumir, compensar o corregir. Estas se establecerán de acuerdo con el nivel de cada riesgo, de acuerdo con lo establecido en la metodología.

Para riesgos de integridad pública las opciones de tratamiento son: Evitar o prevenir.

- **Monitoreo y Seguimiento**

La primera línea de defensa realiza el monitoreo periódico de los riesgos a su cargo, incluyendo los de integridad pública. La segunda línea consolida y elabora el informe de monitoreo con semáforo de KRI institucionales, y el informe periódico para el CICCI y CIGD. Los líderes de los subsistemas del SIG y el responsable con función de cumplimiento monitorean los riesgos a su cargo y reportan al Grupo de Planeación. La tercera línea (Control Interno) realiza el seguimiento y evaluación conforme a la normativa y al Plan Anual de Auditoría.

7. NIVEL DE MADUREZ EN GESTIÓN DEL RIESGO – ANCP-CCE

El nivel de madurez en la gestión de riesgos permite evaluar el grado de desarrollo, implementación y consolidación de las prácticas institucionales en esta materia, así como identificar oportunidades de mejora. En la ANCP-CCE, este análisis se integra como un componente del modelo de gestión adoptado, basado en los cinco componentes y veinte principios del marco COSO-ERM. Como resultado de su aplicación en el primer trimestre del 2026, se obtuvo una calificación del nivel de madurez de 3,9 – definido, lo cual indica que la entidad cuenta con una política de riesgos formalmente establecida, lineamientos claros y procesos documentados. La gestión de riesgos está estandarizada y se aplica de manera más uniforme, alineándose con referentes como ISO 31000 y COSO, aunque aún puede carecer de

medición sistemática de desempeño. Lo anterior se toma como línea base para próximas mediciones.

A continuación, se presenta la calificación obtenida por cada componente:

Componente COSO-ERM	Calificación	Aspectos de mejora identificados
Gobierno y Cultura	3,8	• Fortalecer la **apropiación de la cultura de riesgos** en todos los niveles (no solo directivos). • Aumentar la **participación activa del comité de riesgos** en decisiones estratégicas. • Implementar mecanismos para **medir la cultura organizacional frente al riesgo** (encuestas, indicadores de conducta).
Estrategia y Definición de Objetivos	3,9	• Formalizar y socializar el **apetito y tolerancia al riesgo**. • Integrar explícitamente los riesgos en la **planeación estratégica y operativa**. • Fortalecer la evaluación de **escenarios y alternativas estratégicas** con enfoque de riesgo.
Desempeño (Identificación y Evaluación de Riesgos)	4,4	• Evolucionar hacia analítica más avanzada (riesgos emergentes, predictivos). • Fortalecer la **evaluación del riesgo residual** y su impacto en resultados. • Integrar mejor la gestión de riesgos con indicadores de desempeño institucional.
Revisión y Monitoreo	3,7	• Implementar **monitoreo continuo** con indicadores clave de riesgo (KRIs). • Fortalecer la **evaluación de cambios significativos** del entorno. • Integrar herramientas tecnológicas para seguimiento en tiempo real.
Información, Comunicación y Reporte	3,9	• Mejorar la **oportunidad y claridad de los reportes** para la alta dirección. • Integrar sistemas de información que permitan **visualización y trazabilidad de riesgos**. • Fortalecer la **comunicación bidireccional** (de arriba hacia abajo y viceversa).
RESULTADO GLOBAL	**3,9**	**Meta 2026: 5**

Aspectos Positivos

- ✓ Se evidencia una estructura organizacional clara, con roles definidos, compromiso institucional y desarrollo de capacidades. La cultura de riesgos está en proceso de consolidación.
- ✓ Existe claridad en el contexto institucional y en la definición de objetivos.
- ✓ La entidad ya **identifica, evalúa y responde a los riesgos**, con controles efectivos y priorización adecuada. Se evidencia seguimiento y gestión activa.
- ✓ Se realizan actividades de seguimiento y revisión.

El diagnóstico se aplica de manera anual durante el primer trimestre de cada vigencia, con el propósito de medir la evolución del nivel de madurez, identificar brechas y priorizar acciones de mejora. Los resultados y recomendaciones derivadas de este ejercicio deben ser presentados al CICCI, con el fin de orientar la toma de decisiones y fortalecer continuamente la gestión del riesgo en la entidad.

8. MODELO INTEGRAL DE GESTION DE RIESGOS

La Agencia Nacional de Contratación Pública – Colombia Compra Eficiente (ANCP-CCE) adopta la gestión integral de riesgos con un enfoque multinivel, el cual permite identificar, analizar, evaluar, tratar y monitorear los riesgos de manera articulada en los diferentes niveles de la gestión institucional, garantizando su alineación con los objetivos estratégicos, el modelo de operación por procesos y la gestión institucional.

8.1 NIVELES DE APLICACIÓN DEL SISTEMA INTEGRADO DE RIESGOS

Este enfoque reconoce que los riesgos se identifican y gestionan en distintos niveles de la entidad, los cuales se encuentran interrelacionados y requieren una gestión diferenciada, pero coherente e integrada que permita asegurar el cumplimiento de los objetivos institucionales y la generación de valor público.

Este modelo se estructura en tres niveles:

- **Nivel estratégico**

Corresponde al nivel en el cual se definen el direccionamiento estratégico, los objetivos institucionales, las políticas, los planes, programas y proyectos de la Agencia.

En este nivel se gestionan:

- Riesgos estratégicos asociados al cumplimiento de los objetivos institucionales
- Riesgos que afectan la sostenibilidad institucional y la generación de valor público

- Riesgos asociados a planes, programas y políticas institucionales

Estos riesgos se caracterizan por:

- Alto impacto potencial en la Entidad
- Alta incertidumbre y limitada información histórica
- Baja frecuencia o difícil estimación de ocurrencia
- Influencia directa en la toma de decisiones de la alta dirección

Su gestión permite anticipar y mitigar situaciones que puedan afectar el cumplimiento de la misión, la visión y los objetivos institucionales, fortaleciendo la toma de decisiones y la capacidad de adaptación de la Agencia frente a cambios del entorno.

- **Nivel táctico**

Corresponde al nivel de los procesos, productos y servicios donde se gestionan:

- Riesgos asociados a procesos
- Riesgos asociados a productos y servicios

Estos riesgos se caracterizan por:

- Impacto en el desempeño de los procesos
- Relación directa con el cumplimiento de objetivos de procesos y resultados institucionales (generación de productos y servicios)
- Disponibilidad de información para su análisis y gestión
- Capacidad de intervención mediante controles de proceso

Su gestión permite asegurar la eficiencia, eficacia y efectividad de los procesos institucionales, así como la adecuada prestación de los servicios y la generación de productos en cumplimiento de los objetivos definidos.

- **Nivel operativo**

Corresponde al nivel de ejecución de actividades, tareas y gestión de recursos, en el cual se desarrollan las operaciones diarias de la Entidad.

En este nivel se gestionan:

- Riesgos asociados a actividades rutinarias
- Riesgos asociados a activos (información, talento humano, infraestructura, entre otros)
- Riesgos específicos de los Subsistemas de gestión (SST, ambiental, seguridad de la información, entre otros)

Estos riesgos se caracterizan por:

- Mayor frecuencia de ocurrencia
- Impacto directo en la operación
- Mayor nivel de control y capacidad de intervención

Su gestión permite prevenir fallas operativas, incidentes y desviaciones en la ejecución de las actividades.

8.2 GOBERNANZA DEL RIESGO – ROLES Y RESPONSABILIDADES

En la ANCP-CCE, la gobernanza del riesgo se entiende como el conjunto de estructuras, procesos y mecanismos de control que garantizan la identificación, gestión, monitoreo y comunicación integral de los riesgos en toda la entidad. En este contexto, y en concordancia con el modelo de Líneas de Defensa del MIPG, a continuación, se presentan las responsabilidades definidas para la gestión del riesgo:

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. (CICI) • 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.

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
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. • 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. • 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.

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
		• Acompañar, orientar, entrenar y establecer con los líderes de procesos la identificación, análisis y valoración de los riesgos. • 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. • Coordinar los KRI institucionales y generar alertas tempranas. • Articular la gestión del SIGRIP: debida diligencia, función de cumplimiento, canal de denuncias. • Elaborar el informe consolidado anual del Sistema Integrado de Gestión de Riesgos.
	Responsable de la función de Cumplimiento	• Administrar el Sistema Integrado de Gestión de Riesgos y de Integridad Pública adoptado por la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente. • Articular la definición e implementación de lineamientos institucionales sobre la función de cumplimiento, que permita fortalecer los mecanismos de debida diligencia y la detección de operaciones inusuales o sospechosas, asegurando su coherencia con el modelo de gestión institucional y las directrices de la Alta Dirección. • Promover la definición y mantenimiento de los lineamientos institucionales para el reporte de operaciones sospechosas a la Unidad de Información y Análisis Financiero o entes de control, estableciendo criterios y roles, en coherencia con las disposiciones normativas vigentes.
	Responsables de Sistemas de	• Asegurar la correcta identificación y tratamiento de riesgos especializados.

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
	Gestión (SST, Ambiental, Seguridad de la Información, etc.) (Segunda Línea) Líderes de políticas institucionales	• Garantizar la aplicación de metodologías específicas (ej. jerarquía de controles en SST). • Articular los riesgos de su sistema con la metodología institucional. • Realizar el monitoreo como segunda línea de defensa a los riesgos asociados al sistema de gestión o modelo referencial aplicable. • 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]
Tercer 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, incluyendo los de corrupción y SIGRIP. • 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 estos. • Revisar el perfil de riesgo inherente y residual por cada proceso, así como el perfil 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 no sea coherente con los resultados de las auditorías realizadas. • Llevar a cabo el seguimiento a los riesgos consolidados en el mapa de riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados al CICCI.
Servidores(as) y contratistas	Todos	• Aplicar los lineamientos de gestión del riesgo en el desarrollo de sus actividades. • Reportar riesgos, incidentes o eventos materializados.

[1] Modelo de Seguridad y Privacidad de la Información

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
		• Contribuir activamente a la cultura de autocontrol, integridad y transparencia. • Utilizar el canal de denuncias del SIGRIP cuando identifiquen situaciones que afecten la integridad.

Fuente: Elaboración Propia

8.3 TIPOLOGÍA DEL RIESGO

La ANCP-CCE adopta un enfoque integrado para la gestión de las diferentes tipologías de riesgo, evitando su tratamiento aislado y promoviendo su articulación bajo un único marco metodológico.

Las tipologías de riesgo incluyen, entre otras:

Tabla 2 Tipologías de Riesgos

Tipología	Descripción
Riesgos de gestión	Asociados a procesos, cumplimiento de metas, eficiencia y desempeño institucional.
Riesgos de integridad pública (corrupción-soborno, conflicto de intereses)	Uso indebido del poder; conflictos de interés; desviación de recursos; actos de fraude, actuaciones irregulares, comisión de hechos delictivos, abuso de confianza, apropiación indebida, ofrecer, prometer, entregar, aceptar, solicitar un beneficio o dádiva de manera directa o indirecta. *Nota: Los riesgos de integridad pública (corrupción, fraude, soborno, LA/FT/FP) se gestionan de forma transversal en todas las fases del ciclo del riesgo. Tolerancia cero — solo se evitan o previenen*
Riesgos de integridad pública (LA/FT/FP)	Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva. Análisis basado en factores de riesgo: contrapartes, productos/servicios, canales y jurisdicciones.
Riesgos fiscales	Efecto dañoso sobre los recursos públicos y/o bienes e intereses patrimoniales de naturaleza pública, en los términos de la Ley 610 de 2000.
Seguridad de la información	Pérdida de confidencialidad, integridad o disponibilidad. Accesos no autorizados. Fallas en activos de información. Análisis basado en amenazas, vulnerabilidades y activos (CIA).

Tipología	Descripción
Seguridad y salud en el trabajo	Identificación de peligros, evaluación de riesgos laborales y condiciones inseguras que puedan afectar la salud de funcionarios, contratistas y pasantes.
Riesgos ambientales	Identificación de aspectos e impactos ambientales, considerando intensidad, extensión y reversibilidad. Cumplimiento normativo ambiental.
Continuidad del negocio	Interrupción de servicios críticos o fallas en la operación que afecten la prestación del servicio. Análisis basado en BIA (Business Impact Analysis) y RTO.
Gestión del conocimiento	Pérdida de memoria institucional y fuga de conocimiento clave identificado en las dependencias de la entidad.
Gestión documental	Amenazas o situaciones que pueden afectar la autenticidad, integridad, disponibilidad, fiabilidad confidencialidad, trazabilidad, conservación o preservación de los documentos.
Proyectos de inversión	Riesgos identificados conforme a la Metodología General Ajustada (MGA) o lineamientos del DNP, articulados con este sistema.

Fuente: Elaboración Propia

Consideración general de articulación

- Cada uno de estos riesgos deberá ser identificado bajo la estructura definida en la presente metodología, evitando la generación de metodologías paralelas.
- Cada tipología podrá tener particularidades en su tratamiento; sin embargo, todas deben gestionarse bajo los lineamientos establecidos en la presente metodología, garantizando consistencia, comparabilidad y trazabilidad.
- Independientemente de su tipología o del marco metodológico específico que les aplique, todos los riesgos deberán:
  - Ser estructurados conforme a los lineamientos definidos en la presente metodología
  - Ser registrados en la matriz institucional de riesgos
  - Permitir su trazabilidad, monitoreo y seguimiento
  - Articularse con los procesos de planeación, evaluación y mejora institucional.

- **Riesgos de proyectos de inversión**

Los riesgos asociados a proyectos de inversión deberán identificarse de conformidad con la Metodología General Ajustada (MGA) o los lineamientos definidos por el Departamento Nacional de Planeación (DNP).

No obstante, la gestión de estos riesgos debe articularse documentalmente con la presente metodología para efectos de su consolidación, monitoreo y seguimiento a nivel institucional, garantizando su integración con el Sistema integrado de Gestión de riesgos.

- **Riesgos asociados a procesos contractuales**

Los riesgos asociados a la gestión contractual deberán identificarse y gestionarse de conformidad con la metodología definida por la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente (ANCP-CCE) para la gestión del riesgo en los procesos contractuales.

8.4 ESTRUCTURA DEL RIESGO

En el marco de la presente metodología, el riesgo se estructura como la posibilidad de que un evento ocurra y afecte el cumplimiento de los objetivos, considerando los siguientes elementos:

- Nivel de aplicación del riesgo: estratégico, táctico u operativo.
- Objeto de análisis: objetivo institucional, proceso, producto, activo o actividad.
- Objetivo específico / Activo específico / Aspecto ambiental / Tipo de peligro.
- Evento de riesgo: situación que puede ocurrir y generar afectación.
- Causa raíz e inmediata: por qué puede ocurrir.
- Consecuencias o impactos: efectos de la materialización.
- Tipo de riesgo: clasificación según su naturaleza.

Esta estructura permite una adecuada identificación, análisis y tratamiento del riesgo, facilitando la definición de controles efectivos y un adecuado tratamiento.

- **Criterios de clasificación y priorización**

Los riesgos se clasifican y priorizan considerando criterios que permiten su adecuada gestión, tales como:

- Nivel de impacto
- Probabilidad de ocurrencia
- Nivel de control existente
- Alineación con objetivos institucionales
- Nivel de exposición al riesgo

La criticidad y prioridad de intervención de los riesgos se determina a partir de la valoración integral de estos criterios, considerando especialmente el nivel de riesgo residual resultante de la aplicación de controles. Los riesgos ubicados en zonas de

riesgo **Extrema** y **Alta** serán objeto de atención prioritaria y requerirán la definición e implementación de medidas de tratamiento. Así mismo, se tendrán en cuenta los criterios de apetito y tolerancia al riesgo definidos por la entidad y las particularidades de cada tipología de riesgo.

Estos criterios permiten establecer niveles de riesgo y definir prioridades de intervención.

8.5 GESTIÓN DE RIESGOS EMERGENTES

Los riesgos emergentes corresponden a aquellos riesgos nuevos o en evolución y que se caracterizan por alta incertidumbre y limitada información histórica. Pueden identificarse en el marco del seguimiento a la gestión institucional y pueden presentarse en cualquiera de los niveles de la gestión institucional (estratégico, táctico u operativo) dependiendo de su naturaleza y del ámbito en el que se originen.

La identificación y gestión de los riesgos emergentes es responsabilidad de la primera línea de defensa, quienes deberán reportar oportunamente aquellos eventos, tendencias o situaciones que puedan representar riesgos nuevos o en evolución para la entidad.

La segunda línea de defensa, consolida y analiza la información reportada, coordinar su seguimiento y presenta los resultados ante el Comité Institucional de Coordinación de Control Interno - CICCI.

Características

- Alta incertidumbre
- Información limitada o en desarrollo
- Dinámica cambiante
- Dificultad de cuantificación

Gestión de los riesgos emergentes

La gestión de los riesgos emergentes contempla:

- Identificación y análisis del riesgo
- Registro en instrumentos definidos para su seguimiento
- Análisis cualitativo preliminar
- Clasificación según nivel de impacto y nivel organizacional
- Monitoreo continuo

Los riesgos emergentes serán objeto de revisión como mínimo durante los ejercicios periódicos de monitoreo institucional del riesgo o cuando se presenten cambios significativos en el contexto interno o externo de la entidad.

Para su monitoreo podrán emplearse, entre otros mecanismos:

- Análisis del contexto estratégico e institucional.
- Seguimiento a cambios normativos o regulatorios.
- Alertas sectoriales y reportes de organismos de control.
- Resultados de auditorías internas y externas.
- Indicadores clave de riesgo (KRI).
- Reporte de incidentes, eventos materializados y lecciones aprendidas.

Un riesgo emergente deberá ser escalado para evaluación por la línea estratégica cuando:

- Pueda afectar el cumplimiento de objetivos estratégicos institucionales.
- Su impacto potencial sea catalogado como alto o extremo.
- Genere exposición significativa en materia financiera, reputacional, legal, tecnológica o de integridad pública.
- Requiera la asignación de recursos extraordinarios o decisiones de nivel directivo.

Como resultado de su evaluación, el riesgo emergente podrá mantenerse en observación, incorporarse al mapa institucional de riesgos o ser gestionado como un riesgo estratégico de la entidad.

9. METODOLOGÍA PARA LA GESTIÓN DEL RIESGO

De conformidad con el modelo definido, la gestión del riesgo se basa en un enfoque sistemático, estructurado e integral, que permite la identificación, análisis, evaluación, tratamiento, monitoreo de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales.

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 Faces para la administración de riesgos

Fuente: Elaboración Grupo de Planeación ANCP-CCE

Cada una de estas fases se desarrolla a continuación:

9.1. FASE 1 - IDENTIFICACIÓN DEL CONTEXTO EN LA GESTIÓN DE RIESGOS

El establecimiento del contexto corresponde a la etapa inicial de la gestión del riesgo, en la cual se analizan los factores internos y externos que pueden influir en el cumplimiento de los objetivos institucionales.

En Colombia Compra Eficiente el contexto se construye a partir de los ejercicios de planeación estratégica e institucional, en los cuales se definen los elementos clave del entorno interno y externo de la Entidad.
Para el análisis del contexto, la Entidad podrá apoyarse en las metodologías, herramientas e instrumentos definidos en el proceso de Direccionamiento Estratégico y en los ejercicios de planeación institucional vigentes, tales como análisis del entorno, análisis estratégico, evaluación de factores internos y externos u otras metodologías que permitan identificar elementos relevantes para la gestión del riesgo.

A partir de la identificación o actualización del contexto, se pueden identificar los factores de riesgo que pueden dar origen a eventos que afecten el cumplimiento de los objetivos, permitiendo una gestión del riesgo más pertinente y alineada con la realidad institucional.

9.1.1. CONTEXTO EXTERNO

En la ANCP-CCE, el contexto externo se define a partir de lo establecido en el proceso CCE-DES-CP-01 Direccionamiento estratégico, el MIPG y los modelos internacionales. Esto a partir de los ejercicios de planeación estratégica e institucional, en los cuales se analizan las condiciones del entorno que pueden incidir en la gestión institucional. Para efectos de la gestión del riesgo, estos factores deberán ser analizados y considerados de acuerdo con el nivel en el cual se gestiona el riesgo (estratégico, táctico u operativo).

Entre los principales factores a considerar se encuentran:

- Cambios normativos y regulatorios
- Condiciones económicas y fiscales
- Entorno político e institucional
- Avances tecnológicos
- Factores sociales y ambientales
- Dinámica del mercado de compras públicas
- Relación con grupos de valor y partes interesadas

Este análisis permite identificar factores externos que pueden constituirse en fuentes de riesgo o generar cambios en la exposición al riesgo de la Entidad.

9.1.2. CONTEXTO INTERNO

En la ANCP-CCE, el contexto interno se define en el marco de los ejercicios de planeación institucional, y para efectos de la gestión del riesgo, estos elementos deberán ser considerados de acuerdo con el alcance del análisis definido y el nivel en el cual se gestiona el riesgo (estratégico, táctico u operativo).

Entre los principales factores a considerar se incluyen:

- Estructura organizacional
- Modelo de operación por procesos
- Recursos (humanos, tecnológicos, financieros y físicos)
- Cultura organizacional
- Sistemas de información
- Políticas, lineamientos y procedimientos internos
- Capacidades institucionales y nivel de madurez de los procesos

9.2. FASE 2 - IDENTIFICACIÓN DEL RIESGO

La identificación del riesgo tiene como propósito reconocer y describir los eventos potenciales que pueden afectar el cumplimiento de los objetivos institucionales, así como sus causas y consecuencias, permitiendo establecer una base sólida para su análisis, evaluación y tratamiento.

Esta fase constituye el punto de partida de la gestión del riesgo y debe desarrollarse de manera sistemática, estructurada y articulada con el direccionamiento estratégico, el modelo de operación por procesos y las demás dimensiones del Modelo Integrado de Planeación y Gestión (MIPG). Esta se desarrolla con base en el análisis del contexto interno y externo, el alcance definido y las características del objeto de análisis, permitiendo reconocer de manera estructurada los riesgos en los diferentes niveles de la Entidad (estratégico, táctico y operativo).

9.2.1. Alcance de la identificación

La identificación de riesgos en la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente se realizará de manera integral, considerando:

- **Fuentes internas**
  - Procesos
  - Recursos (humanos, tecnológicos, financieros)
  - Cultura organizacional
  - Fallas en controles
  - Gestión de la información
  - Activos de Información
  - Infraestructura

- **Fuentes externas**
  - Cambios normativos
  - Condiciones del entorno económico
  - Factores políticos o institucionales
  - Avances tecnológicos
  - Factores ambientales
  - Actuación de terceros (proveedores, ciudadanos, aliados)

Estos factores pueden constituirse en causas potenciales de los eventos de riesgo.

- Así mismo, se deben considerar todas las tipologías de riesgo aplicables, incluyendo riesgos de gestión, integridad pública (corrupción - soborno, conflicto de intereses, (LA/FT/FP)), fiscales, de seguridad de la información, de seguridad y salud en el trabajo, ambientales, de continuidad del negocio, de gestión documental, de gestión del conocimiento, entre otros.

9.2.2. Elementos para la identificación del riesgo

La identificación del riesgo deberá realizarse considerando los elementos definidos en la estructura del riesgo (Capítulo 6):

- Nivel de aplicación del riesgo
- Objeto de análisis
- Objetivo o condición asociada
- Evento de riesgo
- Causa raíz e inmediata
- Consecuencias o impactos
- Tipo de riesgo

La correcta identificación de estos elementos garantiza la trazabilidad del riesgo y su adecuada gestión en los diferentes niveles de la Entidad.

9.2.3. Identificación de riesgos por tipologías y sistemas de gestión.

La identificación del riesgo deberá considerar las particularidades de las diferentes tipologías de riesgo y sistemas de gestión adoptados por la Entidad, garantizando su integración en el SIGRIP.

Tabla 3 Particularidades por tipología

Tipo de riesgo	Asociado a:	Aspectos Clave
Riesgos de gestión	• Incumplimiento de metas y objetivos institucionales • Fallas en la ejecución de procesos • Ineficiencias operativas que afecten el desempeño	• El evento debe ser medible o verificable en la operación
Riesgos de integridad pública (corrupción - Soborno, Fraude y conflicto de interés)	• Uso indebido del poder en el ejercicio de funciones • Conflictos de interés que afecten la imparcialidad • Desviación o apropiación indebida de recursos • Actos de fraude, conductas irregulares o comisión de hechos delictivos (abuso de confianza, apropiación indebida, entre otros)	• El evento debe evidenciar uso indebido del poder o desviación del interés público
Riesgos de integridad pública (LA_FT_FP)	• Uso de la entidad para ocultar o dar apariencia de legalidad a recursos de origen ilícito • Canalización de recursos hacia actividades relacionadas con	• El evento debe reflejar una posible materialización observable (transacción, vínculo, operación)

	financiación del terrorismo o proliferación • Vinculación con personas o entidades relacionadas con actividades de LA/FT/FP • Realización de operaciones inusuales o sospechosas	
Riesgos fiscales	• El riesgo fiscal se define de la siguiente manera: Efecto dañoso sobre recursos, bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial**.** Riesgo Fiscal = Evento Potencial (Potencial Conducta) + Efecto dañoso (Potencial Daño) **Evento Potencial:** hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos, los bienes y/o los intereses patrimoniales de naturaleza pública. **Efecto dañoso**: es el daño que se generaría sobre los recursos, los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.	• El evento debe permitir inferir posible detrimento, pero no ser el detrimento en sí. • Identificar puntos de riesgo y circunstancias inmediatas. • Identificar el área de impacto • Identificar el efecto económico. • Identificar la causa raíz. • Describir el Riesgo Fiscal.
Seguridad de la información	• Pérdida de confidencialidad, integridad o disponibilidad de la información • Acceso no autorizado a la información • Interrupción o falla de los sistemas de información	• El evento debe ser medible y trazable
Seguridad y salud en el trabajo	• Ocurrencia de accidentes de trabajo o enfermedades laborales • Exposición de los trabajadores a condiciones inseguras • Materialización de incidentes que afecten la integridad física o la salud	• El evento debe ser una situación que impacta al trabajador
Riesgos ambientales	• Generación de impactos ambientales negativos derivados de la operación • Incumplimiento de requisitos legales ambientales • Afectación de los recursos naturales o del entorno	• El evento debe reflejar una afectación ambiental concreta
Continuidad del negocio	• Interrupción de servicios o procesos críticos	• El evento debe ser una ruptura de la operación

	• Indisponibilidad de recursos necesarios para la operación • Suspensión o afectación de la prestación del servicio	
Gestión del conocimiento	• Pérdida de conocimiento crítico institucional • Dependencia de personas clave para la operación • Dificultades en la transferencia o retención del conocimiento	• El evento debe evidenciar afectación a la continuidad del saber
Gestión documental	• Pérdida de documentos • Alteración no autorizada de la información documental • Indisponibilidad de documentos para la operación o consulta • Pérdida o destrucción de documentos • Alteración o corrupción de la información • Acceso o divulgación no autorizada • Indisponibilidad de documentos • Deterioro físico o digital a largo plazo.	• El evento debe ser verificable en los sistemas o archivos institucionales, y enfocarse en pérdida, alteración o indisponibilidad documental

Fuente: Elaboración Propia

9.3. ESTRUCTURA PARA LA REDACCIÓN DEL RIESGO

Con el fin de garantizar la calidad, consistencia y comparabilidad en la identificación de los riesgos, la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente (ANCP-CCE) establece que el riesgo deberá definirse a partir de la identificación clara del evento de riesgo, entendido como la situación que puede ocurrir y que afecta el cumplimiento del objetivo o condición asociada.

Todo riesgo debe formularse bajo la siguiente estructura:

"Puede ocurrir [evento de riesgo], debido a [causas], lo que generaría [consecuencias]". Cada elemento se registra de forma independiente en la matriz institucional.

De acuerdo con las diferentes tipologías debe considerarse la siguiente redacción:

Tipología	Regla particular de redacción	Ejemplo de redacción del evento de riesgo
Riesgos de gestión	• La redacción debe describir **eventos que afecten el cumplimiento de objetivos**, metas, procesos o la prestación del servicio. Deben	• Incumplimiento de los tiempos de respuesta establecidos en la atención de solicitudes.

	formularse como hechos específicos y verificables.	
Riesgos de integridad pública (corrupción – soborno)	• La redacción debe **evidenciar una acción u omisió**n asociada al uso indebido del poder o desviación del interés público **para beneficio propio o de un tercero**. • Para los riesgos de Corrupción y sus manifestaciones específicas como soborno, fraude e inadecuada gestión del conflicto de intereses, se deben tener en cuenta los puntos de riesgos que pueden ser cualquier actividad dentro del flujo de proceso y no solo las operaciones. • Para conflicto de interés hace relación a la decisión en un asunto sobre el cual el servidor tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tuviere su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho.	• Posibilidad de **aceptar, ofrecer, prometer, entregar, aceptar o solicitar** una ventaja indebida en la designación de citas a favor de un tercero
Riesgos de integridad pública (corrupción - fraude)		• Posibilidad de **modificar** un estudio previo para beneficio propio o a favor de un tercero.
Riesgos de integridad pública (conflicto de interés)		• Posibilidad de **usar información privilegiada** para favorecer a un tercero
Riesgos de integridad pública (LA/FT/FP)	• La redacción debe **enfocarse en operaciones, transacciones, vinculaciones o uso de recursos que puedan asociarse a LA/FT/FP**, describiendo situaciones observables y verificables.	•Posibilidad de contratar de proveedores relacionados con actividades asociadas a LA/FT.
Riesgos fiscales	• La redacción debe **reflejar el** efecto dañoso sobre recursos, bienes y/o intereses patrimoniales de naturaleza pública, a causa de **un evento potencial**.	•Posibilidad de efecto dañoso sobre **los recursos de la entidad** por la generación de intereses moratorios en contrato de arrendamiento.
Seguridad de la información	• La redacción debe orientarse a eventos que afecten la confidencialidad, integridad o disponibilidad de la información y los sistemas institucionales.	•Acceso no autorizado a sistemas de información institucional.
Seguridad y salud en el trabajo	• La redacción debe describir situaciones que puedan afectar la integridad física o la salud de los trabajadores en el desarrollo de sus actividades.	•Ocurrencia de accidentes de trabajo durante la jornada institucional.

Riesgos ambientales	• La redacción debe enfocarse en eventos que generen impactos ambientales negativos derivados de la operación o el incumplimiento de obligaciones ambientales.	•Vertimiento inadecuado de residuos generados en la operación institucional.
Continuidad del negocio	• La redacción debe reflejar interrupciones, indisponibilidad o afectaciones sobre procesos, servicios o recursos críticos para la operación.	•Interrupción del servicio de la plataforma transaccional institucional.
Gestión del conocimiento	• La redacción debe describir situaciones que afecten la conservación, transferencia o disponibilidad del conocimiento crítico institucional.	•Pérdida de conocimiento crítico asociado a procesos estratégicos.
Gestión documental	• La redacción debe enfocarse en eventos que afecten la autenticidad, integridad, disponibilidad, fiabilidad confidencialidad, trazabilidad, conservación o preservación de los documentos.	•Alteración no autorizada de documentos institucionales.

En todos los casos en la matriz institucional, cada uno de estos elementos (**evento, causa, consecuencia**) se registra de manera independiente en los campos definidos para tal fin.

9.3.1. IDENTIFICACIÓN DE CAUSAS Y CONSECUENCIAS

La adecuada identificación de las causas y consecuencias de los riesgos es un elemento clave para una gestión efectiva, ya que permite comprender tanto el origen de los eventos como sus posibles efectos sobre el cumplimiento de los objetivos institucionales. A continuación, se presentan los lineamientos que orientan la identificación y redacción de las causas y consecuencias de los riesgos en la entidad.

a. Lineamientos para la identificación de causas

- Representar el origen del riesgo
- Ser específicas y controlables en la medida de lo posible
- Ejemplos de redacción de las causas:
- Falta de mantenimiento de la infraestructura tecnológica
- Deficiencias en la capacitación del personal
- Ausencia de controles de acceso

b. Lineamientos para la identificación de consecuencias o efectos

- Representar los efectos de la materialización del evento
- Estar alineadas con el impacto sobre los objetivos
- Permitir su posterior valoración (impacto)
- Las consecuencias podrán clasificarse, entre otras, en:
- Operativas
- Financieras
- Reputacionales
- Legales
- Ambientales
- Seguridad y salud en el trabajo
- Seguridad de la información

La especificidad en la gestión de riesgos asociada a los diferentes sistemas de gestión y modelos referenciales adoptados por la Entidad se desarrollará en los capítulos correspondientes del presente documento.

9.4. ANÁLISIS DEL RIESGO

El análisis del riesgo corresponde a la fase en la cual se determina la naturaleza del riesgo y se establecen los niveles de probabilidad de ocurrencia y de impacto de sus consecuencias, con el fin de estimar el nivel de riesgo, lo que permite comprender la magnitud del riesgo, identificar sus principales características y establecer una base técnica para su evaluación y posterior tratamiento.

El análisis del riesgo se realiza sobre los riesgos identificados considerando las particularidades del nivel de aplicación (estratégico, táctico u operativo) y la tipología de riesgo.

9.4.1. ANÁLISIS DE PROBABILIDAD

La probabilidad corresponde a la posibilidad de ocurrencia del evento de riesgo en un periodo determinado y se establece seleccionando un nivel en una escala de muy baja, baja, moderada, alta y muy alta. Para seleccionar la calificación más adecuada se han definido diversos criterios de análisis aplicables de conformidad con el tipo de riesgo identificado:

∴ **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.

Nota: Los criterios detallados de probabilidad por tipología (continua, ocasional, exposición SST, especialización SI, etc.) se encuentran en el Anexo 1 Criterios de valoración de probabilidad del presente manual.

9.4.2. ANÁLISIS DE IMPACTO

El impacto corresponde a 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.

Nota: Estos criterios se encuentran especificados en él y Anexo 2 Criterios para el análisis de impacto – Criterios transversales y Anexo 3. Criterios para el análisis del impacto – criterios específicos del presente manual.

9.4.3. CONSIDERACIONES DIFERENCIALES POR TIPOLOGÍA DE RIESGO

De conformidad con la naturaleza del riesgo, podrán aplicarse criterios específicos para la valoración de la probabilidad y el impacto, en coherencia con los lineamientos de los sistemas de gestión y marcos normativos aplicables.

Entre otros, se podrán considerar los siguientes enfoques diferenciales:

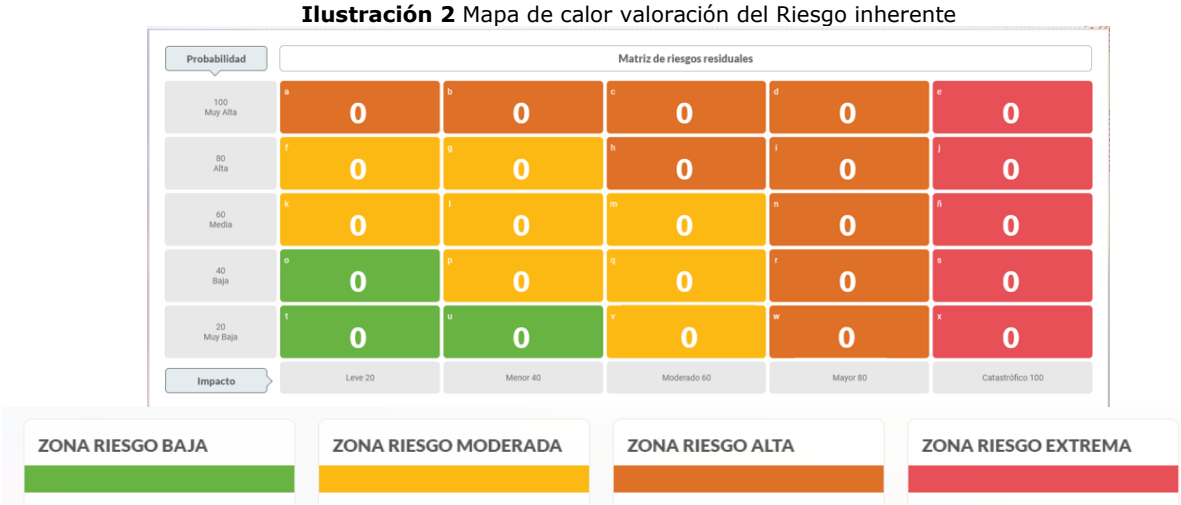
- **Seguridad de la información:**
  Análisis basado en amenazas, vulnerabilidades y activos de información.
- **Seguridad y salud en el trabajo:**
  Evaluación basada en la identificación de peligros, nivel de exposición y severidad del daño.
- **Gestión ambiental:**
  Valoración de aspectos e impactos ambientales, considerando su significancia.
- **Riesgos de corrupción:**
  Análisis basado en factores de oportunidad, presión y racionalización.
- **Riesgos fiscales:**
  Evaluación del posible daño al patrimonio público.

En todos los casos, los resultados del análisis son homologables y compatibles con las escalas definidas en la presente metodología y permitir su consolidación y comparación.

9.4.4. DETERMINACIÓN DEL NIVEL DE RIESGO (RIESGO INHERENTE)

El nivel de riesgo inherente se determina a partir de la combinación de la probabilidad de ocurrencia y el impacto del riesgo, antes de la implementación o considerando la inexistencia de controles. A continuación, se observa el Mapa de Riesgo que utilizará la Agencia en el desarrollo de la Gestión de riesgos.

Ilustración 2 Mapa de calor valoración del Riesgo inherente



Fuente: Suite Vision Empresarial

Este nivel de riesgo permite:

- Identificar riesgos críticos
- Priorizar su gestión

- Establecer la necesidad de tratamiento

9.4.5. IDENTIFICACIÓN DE CONTROLES Y DISEÑO DE CONTROLES.

En el marco del análisis del riesgo, la ANCP-CCE deberá identificar y analizar los controles existentes asociados a cada riesgo, con el fin de determinar su contribución en la mitigación de la probabilidad de ocurrencia y/o del impacto.
Los controles corresponden a las medidas, políticas, procedimientos o mecanismos implementados por la Entidad para prevenir, detectar o corregir la materialización de los riesgos.

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

Tabla 4 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**. **Nota:** Las evidencias en la mayoría de los casos están asociadas con la salida (registro) de las actividades que están señaladas como punto de control de los procedimientos o lo que se establezca en los manuales que este asociado con actividades de revisión, seguimiento, validación, etc.
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**, **algunas veces** o **nunca**, para prevenir, corregir o detectar la materialización de un riesgo según el tipo de control seleccionado previamente. En caso de que el control no sea útil se debe establecer uno nuevo.

Fuente: Elaboración Grupo de Planeación ANCP-CCE

9.5. EVALUACIÓN DEL RIESGO

La evaluación del riesgo corresponde a la fase en la cual se compara el nivel de riesgo identificado (riesgo inherente) con los criterios definidos por la Entidad, en particular con el apetito y la tolerancia al riesgo, con el fin de establecer su nivel de aceptabilidad y definir la necesidad de tratamiento.

Esta etapa permite priorizar los riesgos, orientar la toma de decisiones y establecer las acciones necesarias para su gestión.

9.5.1. CRITERIOS DE EVALUACIÓN DEL RIESGO

La evaluación del riesgo se realiza considerando los siguientes criterios:

- Nivel de riesgo inherente
- Apetito de riesgo definido por la Entidad
- Tolerancia al riesgo
- Nivel de exposición
- Relevancia frente a los objetivos institucionales

Estos criterios permiten determinar el nivel de aceptabilidad del riesgo y su priorización.

9.5.2. APETITO Y TOLERANCIA AL RIESGO

La ANCP-CCE define el apetito de riesgo como el nivel de riesgo que la Entidad está dispuesta a aceptar para el cumplimiento de sus objetivos institucionales.

Para la ANCP-CCE la tolerancia al riesgo corresponde al nivel de desviación permitido respecto al apetito de riesgo, dentro del cual el riesgo puede ser gestionado sin requerir acciones adicionales inmediatas.

En la agencia se establecen los siguientes niveles para determinar la aceptabilidad del riesgo residual:

Nivel	Clasificación	Implicaciones para la gestión
BAJO	Aceptable	Dentro del apetito. Se gestiona con controles existentes y monitoreo periódico.
MODERADO	Tolerable	Supera el nivel óptimo, pero está dentro de la tolerancia. Requiere seguimiento reforzado y posibles acciones de mejora.
ALTO	Inaceptable	Supera apetito y tolerancia. Requiere tratamiento obligatorio, priorización e intervención activa.
EXTREMO	Crítico	No admisible. Requiere intervención inmediata, acciones urgentes e implementación de controles. Reporte obligatorio a la línea estratégica.

Nota sobre Riesgos de Corrupción:
Los riesgos de corrupción tienen tolerancia cero en la ANCP-CCE. Su impacto se califica siempre como MUY ALTO (Extremo) por la gravedad de los efectos que generan, independientemente de su probabilidad de ocurrencia.

9.5.3. CLASIFICACIÓN DEL RIESGO

Como resultado de la evaluación los riesgos se clasifican de acuerdo con su nivel para determinar su aceptabilidad y definir las acciones de gestión correspondientes.

Estos niveles se derivan de la combinación de probabilidad e impacto, de acuerdo con las escalas definidas en los anexos metodológicos.

9.6. 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 5 Opciones de tratamiento de riesgos de acuerdo con la zona de riesgo

Zona de riesgo		Opciones de tratamiento								
		Evitar o prevenir	Reducir - controles Administrativos	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.

- **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.

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.

10. INDICADORES CLAVE DE RIESGO (KRI) INSTITUCIONALES

Los Indicadores Clave de Riesgo (KRI) constituyen una herramienta para el monitoreo y seguimiento de los riesgos, al proporcionar señales oportunas sobre cambios en su nivel de exposición y la efectividad de los controles implementados.

La ANCP-CCE adopta un sistema de KRI institucionales de carácter global, agrupados por tipología de riesgo, orientados a monitorear la exposición del Sistema Integrado de Gestión de Riesgos en su conjunto, y no un KRI individual por cada riesgo del mapa. Este enfoque permite una gestión más eficiente y enfocada en los factores críticos de exposición institucional.

10.1. ESTRUCTURA DE LOS KRI INSTITUCIONALES

Cada KRI institucional se define con los siguientes elementos: nombre del indicador, objetivo de monitoreo, fórmula de cálculo, fuente de datos, umbral de alerta (verde / amarillo / rojo), frecuencia de medición, responsable de medición y línea de reporte:

Tipología / KRI	Descripción / Fórmula	Umbral de Alerta	Frecuencia	Responsable Medición
KRI-G1: % riesgos en zona Alta o Extrema sin plan de tratamiento	(N° riesgos residuales Alto/Extremo sin plan de tratamiento activo / Total riesgos Alto/Extremo) × 100	Verde <10%; Amarillo 10-25%; Rojo >25%	Trimestral	Grupo Planeación (2ª línea)
KRI-G2: % riesgos materializados en el período vs. período anterior	(N° eventos de materialización período actual / N° eventos período anterior) × 100	Verde <10% variación; Amarillo 10-25%; Rojo >25%	Trimestral	Grupo Planeación (2ª línea)
KRI-G3: % riesgos en zona alta o extrema después de aplicación de controles	(N° riesgos residuales Alto/Extremo / Total riesgos inherentes Alto/Extremo) × 100	Verde <40% variación; Amarillo 41-75%; Rojo >75%	Trimestral	Grupo Planeación (2ª línea)
KRI-I1:v , N° denuncias recibidas en el canal de denuncias	Conteo absoluto de denuncias registradas en el período. Tendencia ascendente requiere investigación.	Monitoreo continuo; alerta ante tendencia +50%	Trimestral	Responsable Cumplimiento (SIGRIP)
KRI-I2: % contrapartes con debida diligencia al día	(N° contrapartes activas Alto Riesgo con DD vigente / Total contrapartes activas Alto Riesgo) × 100	Verde >95%; Amarillo 85-95%; Rojo <85%	Semestral	Responsable Cumplimiento
KRI-I3: N° conflictos de interés reportados sin trámite	N° declaraciones de conflicto de interés recibidas con más de 5 días hábiles sin gestión	Verde 0; Amarillo 1-2; Rojo ≥3	Mensual	Responsable Cumplimiento
KRI-SI1: N° incidentes de seguridad de la información en el período	Conteo de incidentes de seguridad registrados y clasificados por severidad (alta, media, baja).	Verde 0 alta/3 media; Amarillo 1 alta; Rojo ≥2 alta	Trimestral	Oficial de Seguridad

Tipología / KRI	Descripción / Fórmula	Umbral de Alerta	Frecuencia	Responsable Medición
KRI-SI2: % activos de información con valoración CIA actualizada	(N° activos con valoración CIA vigente / Total activos registrados) × 100	Verde >90%; Amarillo 75-90%; Rojo <75%	Semestral	Oficial de Seguridad /
KRI-SST1: Tasa de incidentes de trabajo en el período	(N° accidentes/incidentes de trabajo / Total días trabajados en el período) × 10.000	Verde <1.5; Amarillo 1.5-3; Rojo >3	Trimestral	Grupo Talento Humano / SST
KRI-M1: Nivel de madurez COSO-ERM global (% anual)	Resultado del diagnóstico anual de madurez COSO-ERM (5 componentes, 20 principios).	Verde >80%; Amarillo 65-80%; Rojo <65%	Anual	Grupo Planeación (2ª línea)

10.2. REPORTE DE KRI EN EL ESQUEMA DE LÍNEAS

Línea	Instancia de Reporte	Alcance del Reporte KRI
Primera Línea	Segunda línea (Planeación)	Reporte trimestral de monitoreo incluyendo señales de alerta de KRI en sus procesos.
Segunda Línea	CIGD / CICCI	Informe semestral consolidado de KRI institucionales: semáforo por tipología, tendencias, alertas activadas y acciones tomadas.
Tercera Línea	CICCI	Cobertura de los riesgos críticos en las auditorías.
Línea Estratégica	Alta Dirección	Revisión semestral de KRI institucionales para toma de decisiones estratégicas. Activación de umbrales críticos (rojo) genera reporte inmediato a la Alta Dirección.

11. MONITOREO DEL RIESGO

El Monitoreo de Riesgos consiste en realizar una revisión y consolidación de la información reportada por las dependencias, 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 trimestral 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

Una vez consolidada y validada la información la segunda línea de defensa, se elabora el informe del monitoreo y miden los indicadores del Sistema integrado de gestión de riesgos.

De manera anual la segunda línea de defensa elabora un informe consolidado del integrado de gestión de riesgos a partir de la información reportada por la primera línea de defensa en los monitoreos periódicos.

Nota: El enlace de cada dependencia tiene el rol de gestionar y consolidar la información correspondiente al monitoreo de riesgos y el de registrar el reporte periódico en la herramienta establecida para tal fin, así como, de las materializaciones identificadas.

12. 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 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.

13. 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 administración del Sistema de Administración del 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.

Autores y responsables del Documento				
Acción	Nombre	Cargo/ Perfil	Fecha	Firma
Elaboró	Lenny León Walter Silva	Contratistas	14/05/2026	Original Firmado
Revisó	Cesar Andrés Barros de la Ossa	Asesor Experto con funciones de Planeación	26/06/2026	Original Firmado
Aprobó	Comité Institucional de Coordinación de Control Interno - CICCI	Comité Institucional de Coordinación de Control Interno - CICCI	26/06/2026	Acta sesión comité 26de junio de 2026

MANUAL METODOLOGICO PARA LA GESTIÓN INTEGRAL DE RIESGOS

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	Se requieren recursos o habilidades básicas de usuario TI y conocimientos generales del negocio para

						durante la jornada laboral	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

MANUAL METODOLOGICO PARA LA GESTIÓN INTEGRAL DE RIESGOS

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	**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**	**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.**

		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.	**activo que haya sido afectado: confidencialidad, integridad y disponibilidad.**		
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. Menor	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 afecta servicios, procesos o funciones valorados con criticidad MEDIA.	Si el RTO para los servicios, procesos, elementos o funciones críticas y/o sensibles afectados es de 8 a 12 horas.
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	Grado de transformación total, extensión crítica, irreversible	Dos o tres propiedades del activo afectado puntúan como	La interrupción tiene un impacto catastrófico si afecta totalmente alguno	Si el RTO para los servicios, procesos, elementos o funciones críticas y/o

	(con incapacidad permanente o invalidez)		"Información Pública Reservada" o "ALTA".	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.	sensibles afectados es de 0 a 4 horas.