Corporación para el Desarrollo Sostenible del Norte y el Oriente Amazónico

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

(Resolución 092 del 30 de marzo del 2023, consta de 27 folios actualizada)

CONTENIDO

INDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

La política de Administración del Riesgo de la CORPORACIÓN PARA EL DESARROLLO SOSTENIBLE DEL NORTE Y EL ORIENTE AMAZÓNICO CDA se fundamenta en la **Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 de noviembre de 2024**, de acuerdo con los lineamientos para la administración de los riesgos de gestión, integridad, fiscales y seguridad de la información, con un enfoque preventivo y de evaluación permanente de la gestión y el control basado en el mejoramiento continuo, con la participación de todos los líderes de proceso de la entidad.
Además involucra todas las áreas y procesos de la Entidad, teniendo en cuenta el contexto, la identificación, valoración, tratamiento, monitoreo, revisión, comunicación, socialización, consulta y el análisis de los siguientes riesgos:

- Los riesgos de gestión de proceso que puedan afectar el cumplimiento de la misión, los objetivos y proyectos institucionales.
- Los riesgos de integridad asociados a posibles actos de corrupción, orientados a prevenir el uso del poder para desviar la gestión de lo público hacia un beneficio privado.
- Los riesgos fiscales que puedan afectar el patrimonio público como consecuencia de decisiones, acciones u omisiones en la gestión institucional.

La Corporación CDA determina mediante el Sistema Integrado de Gestión Institucional -SIGI y por medio del Procedimiento Administración del Riesgo la identificación, valoración, evaluación los riesgos de gestión, integridad y fiscales, para lo cual la Oficina Asesora de Planeación realiza la actualización de acuerdo con los requerimientos y unificara la información que se dispone al servicio de todos los procesos.
El periodo de revisión e identificación de los riesgos que puedan afectar positiva o negativamente el accionar institucional deberá hacerse atendiendo la metodología vigente, una vez que se defina el plan de acción asegurando la articulación de estos con cada proceso.

1. OBJETIVO

Establecer los lineamientos metodológicos que orienten a la entidad a identificar, valorar, evaluar, y monitorear los diferentes riesgos que puedan tener efectos desfavorables e impactar en el cumplimiento de la misión institucional.

2. ALCANCE

Aplica a todos los procesos, proyectos y servicios de la Entidad, conforme a todas las acciones ejecutadas por los servidores Públicos durante el ejercicio de sus funciones y las tres líneas de defensa.

3. TÉRMINOS Y DEFINICIONES

Activo: En el contexto de seguridad digital 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.

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.

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.

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 Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

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 demás partes interesadas.

Control: Medida que permite reducir o mitigar un riesgo.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Integridad: Propiedad de exactitud y completitud.

Nivel de riesgo: Es el resultado de combinar la **probabilidad** de que ocurra un evento con el **impacto** que tendría sobre el logro de los objetivos institucionales. Generalmente se determina mediante una matriz de probabilidad e impacto o la relación entre ambas variables.

Plan Anticorrupción y de Atención al Ciudadano: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

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.

Riesgo de Integridad: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgo Fiscal: Posibilidad de que, por acción u omisión, se produzca un daño al patrimonio público derivado de una gestión fiscal antieconómica, ineficaz, ineficiente, inequitativa o inoportuna.

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 Inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

Riesgo: 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.

- Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (098) 5 65 63 51 – 5 65 63 52
- Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
- Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel: 310 2 05 80 18
- Website: www.cda.gov.co e-mail: cda@cda.gov.co

Tolerancia del riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.

4. CONTEXTO DE LA ENTIDAD

4.1 Misión

La Corporación CDA es una entidad pública que ejerce la autoridad ambiental en los departamentos de Guainía, Guaviare y Vaupés, bajo la normatividad vigente y el talento humano, lidera la gestión y ejecución participativa de políticas, planes, programas y de proyectos estratégicos de desarrollo ambiental y económico, que contribuyen al conocimiento, la conservación, recuperación, restauración y protección de los recursos naturales y el medio ambiente del Norte y Oriente Amazónico Colombiano, en pro de un desarrollo sostenible para todos.

4.2 Visión

La CDA en el 2030 como autoridad ambiental, será la entidad líder en gestión sostenible, inclusiva del territorio de la región del Norte y Oriente amazónico colombiano, habrá consolidado un modelo ambiental regional viable, prospero, incluyente, equitativo, adaptado, seguro y sostenible, aprovechando la diversidad cultural, geográfica, ecosistémica y productiva, mediante la innovación y el conocimiento, convirtiendo la amazonia como un territorio de oportunidades de desarrollo sostenible para todos. Los procesos, su identificación y relación están ilustrados en el Mapa de Procesos, adoptado mediante resolución 148 del 19 de mayo de 2015 que deroga la resolución 318 del 10 de agosto de 2008 la cual permite entender la distribución de los procesos de la Corporación, y cómo éstos interactúan para atender las necesidades del usuario y transformarlas en satisfacción de todas las partes interesadas (sociedad, medio ambiente, Estado, órganos de control). Adicionalmente, la descripción de cada uno de los procesos está documentada en la caracterización de cada proceso (Estratégicos, Misionales, de Apoyo, Evaluación y Mejora).

4.3 Mapa de Procesos

En cuanto al proceso de Direccionamiento estratégico, este se encarga de formular las directrices e instrumentos de planeación que orienten la gestión de la CDA y a los actores, hacia el logro del mejoramiento de la calidad de vida de los habitantes y la sostenibilidad de los recursos naturales de la jurisdicción.
Dentro de los procesos Misionales tenemos:

- Normatización y Calidad Ambiental; quién se encarga de Consolidar acciones de control, monitoreo, seguimiento, evaluación al igual regular el uso, manejo y aprovechamiento de los recursos naturales que conlleve a garantizar la sostenibilidad en los ecosistemas del norte y oriente amazónico.
- Ordenación y planificación ambiental del territorio; Implementa estrategia de gestión ambiental mediante el ordenamiento gradual del territorio para el conocimiento y planificación del manejo sostenible de los recursos naturales y del medio ambiente en la jurisdicción de la CDA.
- Promoción del Desarrollo Sostenible; se encarga de consolidar actividades para la recuperación y sostenibilidad ambiental del territorio mediante la trasferencia de tecnología e información aplicables a la jurisdicción para la reducción de la presión sobre los Recursos Naturales por intervención antrópica y natural fortaleciendo la cultura ambiental.

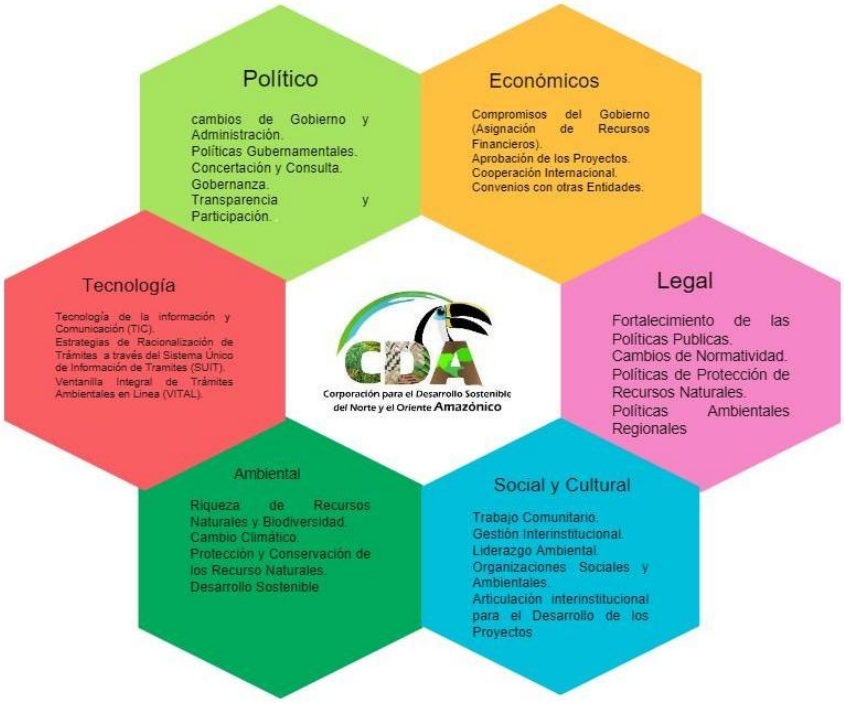
En el marco de los procesos de Apoyo tenemos:

- La Gestión de talento humano; que permite Planear, ejecutar y evaluar estrategias y metodologías para la selección, vinculación, inducción, capacitación, bienestar, compensación, evaluación del desempeño, procesos disciplinarios y retiro de los servidores públicos de la entidad, de manera que se disponga del talento humano idóneo que permita el desarrollo de la misión, visión y objetivos estratégicos institucionales, dentro de un clima organizacional adecuado.
- Gestión de adquisición de bienes y Servicio; se encarga de proporcionar y mantener los bienes muebles e inmuebles de la Corporación, que son necesarios para el logro de las actividades y el cumplimiento de la misión y objetivos institucionales.
- El proceso de gestión documental; se encarga de administrar actividades técnicas tendientes a la planificación, manejo y organización de la documentación producida y recibida por las entidades, desde su origen hasta su destino final, con el objeto de facilitar su utilización y conservación.
- La gestión administrativa y financiera; encargada de definir el procedimiento por el cual se identifica, mide, registra y describe la situación y el resultado de la actividad financiera, económica, social y ambiental de la Corporación.
- El proceso de gestión jurídica; se encarga de representar a la entidad judicialmente y asegurar que las decisiones y actuaciones jurídico-administrativos de la corporación se enmarquen dentro de los parámetros previstos en la normatividad legal vigente.
- El Proceso de Gestión de Bienes e Infraestructura; se encarga de registrar bienes muebles e inmuebles de consumo y/o devolutivo de almacén, para el manejo y control de los mismos; procedimiento que puede darse por adquisición, por compra de caja menor, donaciones, bienes recibidos en comodato, donación en pago, leasing con opción de compra, remesa o traslado entre bodegas o entre entidades, recuperación, reposición, sobrantes, producción, sentencias y por bienes adquiridos dentro del objeto contractual para el desarrollo del mismo(contratos de obra, convenios entre otros) en el cual se especifique q deben ser entregados a la corporación una vez ejecuten el contrato.

En cuanto al proceso de evaluación y mejora; se encarga de evaluar el desarrollo, mantenimiento y mejora del SIGI, administrando de manera eficaz, las herramientas de control interno para asegurar el cumplimiento de las políticas, normas, acuerdos y reglamentos establecidos por los diferentes procesos de la Corporación.

Además, el contexto interno y externo de la entidad parte de abordar otros temas de interés en relación Administración del riesgo está enmarcada en la Manual de calidad V11 4 contexto de la organización.

Figura 1 Contexto



Fuente: Propia de la Entidad, 2023.

5. LINEAMIENTOS DE LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

5.1 Nivel de Responsabilidad.

La Responsabilidad está definida mediante las tres líneas de defensa y en la entidad se acogen de la siguiente manera:

Tabla 1: Responsabilidades de las líneas de Defensa

LÍNEA DE DEFENSA	RESPONSABLE	RESPONSABILIDADES FRENTE AL RIESGO	PERIODICIDAD
Estratégica	Alta dirección Comité institucional de Control Interno	Analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento de los planes estratégicos, así como definir la política de administración del riesgo y el cumplimiento de los planes de la entidad. Aspecto clave: -Definir y evaluar la Política de Administración del Riesgo. La evaluación debe considerar su aplicación en la entidad, cambio en el entorno que puedan definir ajustes, dificultades para su desarrollo, riesgos emergentes.	permanente
Primera Línea	Servidores Públicos en todos los niveles de la entidad	-Mantenimiento efectivo de controles internos, la ejecución de gestión de riesgos y controles en el día a día. Para ello, identifica, evalúa, controla y mitiga los riesgos a través del "Autocontrol". -Identificar riesgos y establecer controles, así como su seguimiento, acorde con el diseño de dichos controles, evitando la materialización de los riesgos.	permanente

		Informar a la Oficina Asesora de Planeación o quien haga sus veces (Como segunda 2 línea de defensa) sobre los riesgos materializados en los procesos, programas, proyectos y planes en su cargo. En caso de la materialización de un riesgo no identificado, este debe ser incluido en el mapa de riesgos del proceso correspondiente. Establecer y aplicar las acciones de mejora requerida frente al mapa de riesgos correspondiente, una vez se genera el informe de materialización del riesgo.	
Segunda Línea	Servidores que Ocupan cargos del nivel directivo asesor (media o alta gerencia), quienes realizan labores de supervisión sobre temas transversales para la entidad y rinde cuentas ante la Alta Dirección Jefe de Planeación, Coordinadores de equipos de trabajo, Coordinadores de Sistema de Gestión. Coordinadores de contratación, financiera y de TIC	Brindar herramientas de apoyo (metodología) a los líderes de los procesos con el fin de facilitar la identificación y evaluación de los riesgos. Asesorar a la primera línea de defensa en la gestión de los riesgos de gestión, integridad, fiscales y de seguridad de la información. Monitorear el cumplimiento de las políticas de gestión de riesgos de gestión, integridad, fiscales y de seguridad de la información. informar a la alta Dirección sobre aquellos riesgos de nivel Critica / Alto, identificados en los Procesos. Monitorear la gestión de los riesgos y oportunidades ejecutada por	Permanente Permanente Gestión: (trimestral) Integridad: (Cuatrimestral) Fiscal (Trimestral) Seguridad de la Información: (Anual). Permanente

		la primera línea de defensa.	

		Asegurar que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende.	
Tercera Línea	Oficina de control Interno.	Desarrollar su labor a través de los siguientes roles: liderazgo, enfoque hace la prevención, evaluación de la gestión del riesgo, relación con entes externos de control y el de evaluación y seguimiento. Emitir observaciones y recomendaciones asociadas al Sistema de Control Interno (SCI) a efectos de reducir y mitigar riesgos identificados. Proporcionar una evaluación independiente y objetiva sobre el diseño y la efectividad de los controles implementados para la mitigación de los riesgos identificados. Verificar el cumplimiento de la política de administración de riesgos y de evaluar la efectividad de los riesgos a través de seguimientos periódicos y auditorias interna desde la tercera línea de defensa. Llevar a cabo la evaluación independiente a los riesgos registrados en los mapas de riesgos de conformidad con el Plan Anual de Auditoria y reportar los	Permanente Trimestral Cuatrimestral Semestral

		resultados al comité Institucional de Coordinación de Control Interno- CICC Asesorar y acompañar a toda la Alta Dirección en la incorporación de estrategias y metodologías para la gestión de riesgos, acorde con las actualizaciones en materia de riesgos de integridad, fiscales, de lavado de activos y otros que se definan en las normas nacionales	

Fuente: Resolución N° 362 del 19 de Noviembre de 2024 anexo Política de control interno *implementación esquema líneas de defensa*

5.2 Comunicación y Socialización de la Política de Gestión del Riesgo

La comunicación y socialización de la Política de Administración de Gestión del Riesgo debe tener en cuenta todas las partes involucradas tanto internamente (líderes de procesos) y externamente (usuarios), facilitando el intercambio de información durante la gestión de los riesgos. Donde la Oficina Asesora de Planeación impulsara mediante capacitaciones, asesorías la apropiación de la política. Además, el mapa de riesgos de integridad será publicado en la página web institucional, en la sección de Transparencia y Acceso a la Información Pública, para consulta de la ciudadanía.

5.3 Seguimiento al Cumplimiento de la Política, Monitoreo y Revisión de los Riesgos

Se realiza el seguimiento, monitoreo y revisión de la Política de Administración del Riesgo de la entidad, de acuerdo con los riesgos de gestión (trimestral), riesgos de integridad (cuatrimestral), riesgos fiscales (trimestal) y riesgos de seguridad de la información (anual), siguiendo los lineamientos establecidos para las tres líneas de defensa.

5.4 Identificación del Riesgo u Oportunidades

Se identifican los riesgos que estén o no bajo el control de la Entidad, por lo cual se tiene en cuenta el Contexto de la Organización, la caracterización de los procesos, el objetivo, el alcance y los factores internos y externos, y las partes interesadas establecidos en el Manual de calidad vigente.

5.4.1 Análisis de Objetivos Estratégicos y de los Procesos

Los riesgos que se identifiquen deben tener un impacto en el cumplimiento del objetivo del proceso. Por lo cual la entidad debe analizar los objetivos de los procesos y revisar que se encuentren alineados con la misión y la visión

institucional.

Por lo cual al iniciar la etapa de identificación de riesgos se utilizan herramientas y técnicas de trabajo con el equipo humano de la Corporación CDA de la siguiente forma:

- Realizar reuniones de trabajo por proceso con los responsables, para la identificación y actualización de los riesgos, en el marco de las líneas de defensa de la entidad.

5.4.2 Descripción del Riesgo de Gestión, Integridad y Fiscal

Debe contener los detalles necesarios que sean necesarios de fácil entendimiento para los líderes de procesos, teniendo en cuenta la siguiente estructura que facilita su redacción y claridad por lo cual se inicia con la frase **POSIBILIDAD DE.**

Figura 2 Estructura para la Redacción del Riesgo de Gestión y Fiscal

Fuente: Manual Metodología de Riesgos, 2022.

Desglosando la estructura propuesta tenemos:

- **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.
  - **Afectación económica:** afectación económica presupuestal de la entidad.
  - **Afectación Reputacional:** afectación de la imagen de la entidad.

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

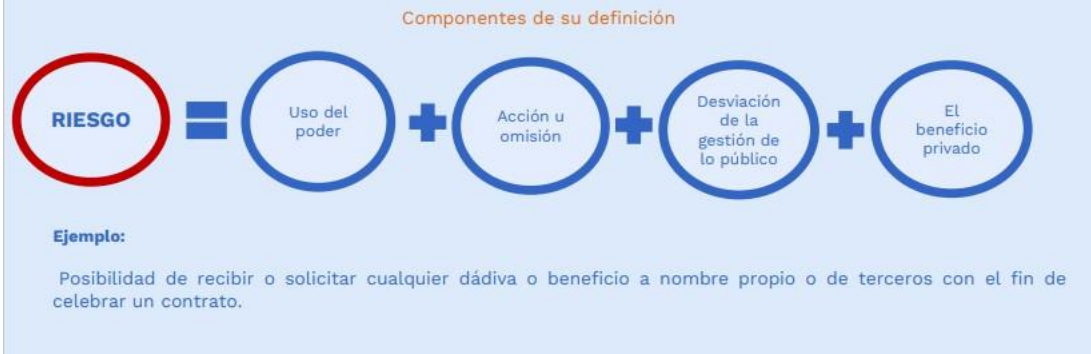
Riesgo de Integridad

Un riesgo de integridad corresponde a la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

> *"esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos" (Conpes N° 167 de 2013).*

Con el fin de facilitar la identificación de los riesgos de integridad y evitar que se presenten confusiones entre un riesgo de gestión y un riesgo de integridad, es necesario que en la descripción del riesgo concurran los componentes de su definición, así:

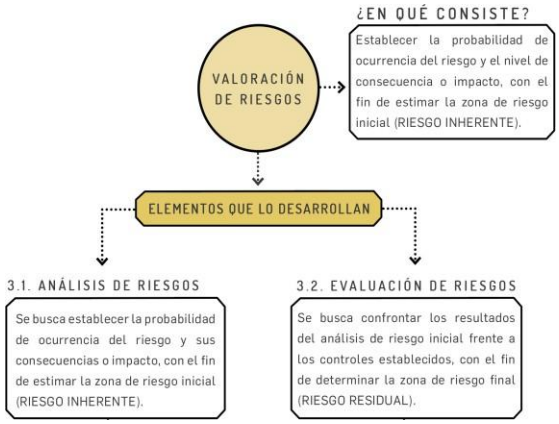
Figura 3 Estructura para la Redacción del riesgo de Integridad



Fuente: Manual Metodología de Riesgos, 2022.

5.5 Valoración del Riesgo de Gestión, Integridad y Fiscal

Figura 4 Estructura para la Valoración del Riesgo



Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2018.

5.5.1 Análisis de Riesgos

Teniendo en cuenta los lineamientos establecidos por el DAFP, en este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias (Probabilidad e impacto), donde la **probabilidad** se entiende como la posibilidad de ocurrencia del riesgo.

En este sentido el nivel de la probabilidad está relacionada a la **exposición al riesgo** la cual se **asocia** al proceso o actividad que se esté analizando, es decir, al **número de veces que se pasa por el punto de riesgo en el periodo de 1 año,** por lo cual la tabla de valoración para la probabilidad de los riesgos tiene en cuenta los siguientes criterios:

Tabla 2 Criterios para definir el nivel de Probabilidad por Gestión

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año.	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año.	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.	100%

Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas V7, 2025

Tabla 3 Criterios para definir el nivel de Probabilidad para Riesgos de Integridad

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	**Probable**	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	**Posible**	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	**Improbable**	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	**Rara vez**	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas V6, 2022

5.5.2 Nivel para Calificar el Impacto

Para la construcción de la tabla de criterios se definen los impactos económicos y reputaciones como variables principales, cada uno con una mayor afectación, cabe aclarar que cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto.

La calificación del impacto de riesgos de Gestión es la siguiente:

Tabla 4 Criterios para definir el Impacto en Riesgo de Gestión

	Afectación Económica (o presupuestal)	Pérdida Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de alguna área de la organización
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta dircetiva y accionistas y/o de provedores
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país

Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas V6, 2022

La calificación del impacto para los riesgos de integridad se realiza aplicando la siguiente tabla de valoración, donde cada riesgo identificado es valorado de acuerdo con las preguntas.

Tabla 5 Criterios para definir los Impactos en riesgos de Integridad

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

Fuente: Secretaría de Transparencia de la Presidencia de la República.

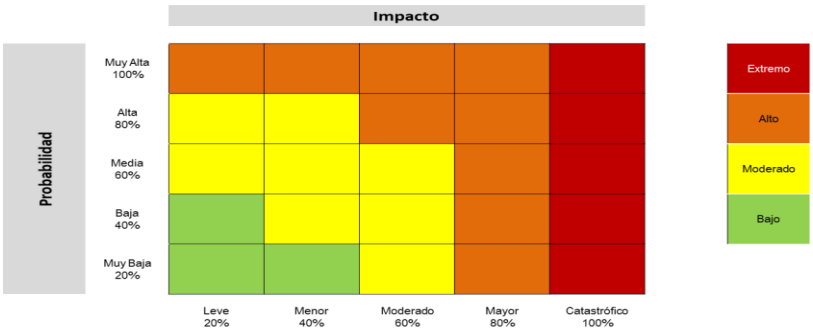
Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas V7, 2025

5.5.3 Evaluación de Riesgos

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la **zona de riesgo inicial (riesgo Inherente).**

Por lo cual se determinan los niveles de severidad a través de la combinación entre la probabilidad y el impacto, por lo cual se definen cuatro (4) zonas de severidad en la matriz de calor.

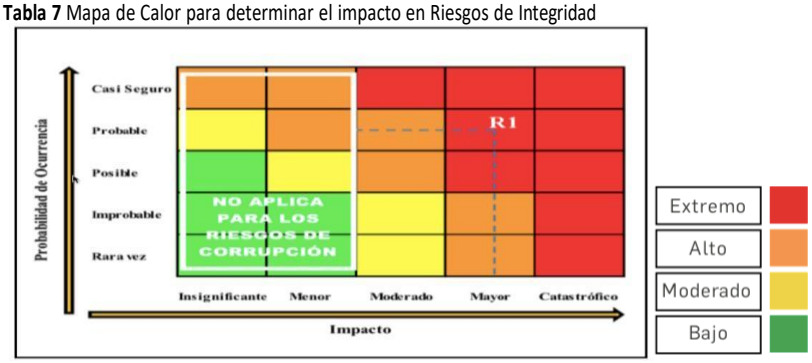
Tabla 6 Mapa de Calor para determinar los niveles de Severidad



Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas V7, 2025

Para los riesgos de Integridad, la tabla **de** probabilidad es la misma que se utiliza para el riesgo de Gestión o Fiscales. Sin embargo, **Para la determinación del impacto frente a posibles materializaciones de riesgos de Integridad,** se analizarán únicamente los siguientes ***n*iveles i) moderado, ii) mayor, y iii) catastrófico,** dado que estos riesgos siempre serán significativos, en tal sentido, no aplican los niveles de impacto insignificante y menor, que sí aplican para las demás tipologías de riesgos.

Tabla 7 Mapa de Calor para determinar el impacto en Riesgos de Integridad

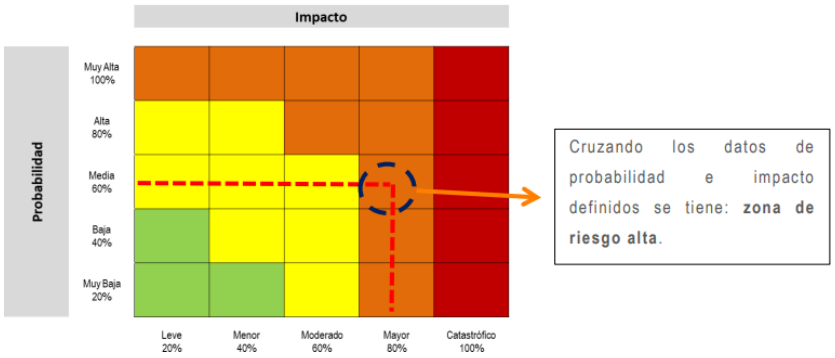


Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas V7, 2025

Una vez determinada la probabilidad (inherente) y el impacto (inherente), se establece el punto de intersección entre ambas, lo cual corresponde al nivel de riesgo inicial (riesgo inherente).

Ejemplo: Probabilidad inherente= Media 60% Impacto
inherente =mayor 80%

Tabla 8 Ejemplo de determinación de la zona de Riesgo Inherente



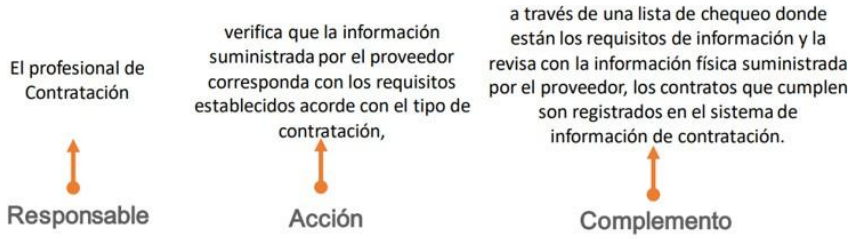
Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas V7, 2025

5.6 Identificación del Control y Valoración del Riesgo Residual

Un control se define como la medida que permite reducir o mitigar el riesgo, la identificación de controles se debe realizar para cada riesgo a través de las entrevistas con los líderes de procesos o servidores públicos. Por lo cual los responsables de implementar y monitorear los controles son los líderes de procesos con el apoyo de su equipo de trabajo. Donde se tiene en cuenta la siguiente estructura para la redacción del control:

- **Responsable de ejecutar el control:** identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
- **Acción:** se determina mediante verbos que indican la acción que deben realizar como parte del control.
- **Complemento**: corresponde a los detalles que permiten identificar claramente el objeto del control.

Figura 5 Ejemplo para la Estructura de la Redacción del Control



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Tipología de controles: a través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión.
Acorde con lo anterior, tenemos las siguientes tipologías de controles:

- **Control preventivo:** control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
- **Control detectivo:** control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- **Control correctivo:** control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

Tabla 9 Atributos para el Diseño de Control

Características			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la	25%

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

- **Control manual:** controles que son ejecutados por personas.
- **Control automático:** son ejecutados por un sistema.

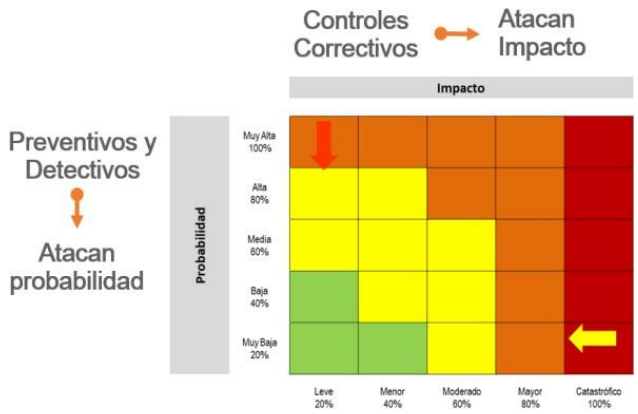
Características			Descripción	Peso
			intervención de personas para su realización.	
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
*Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	-
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas V7, 2025

Los atributos informativos solo permiten dar formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos.

Tabla 10 Movimiento en la Matriz de calor de acuerdo al tipo de control



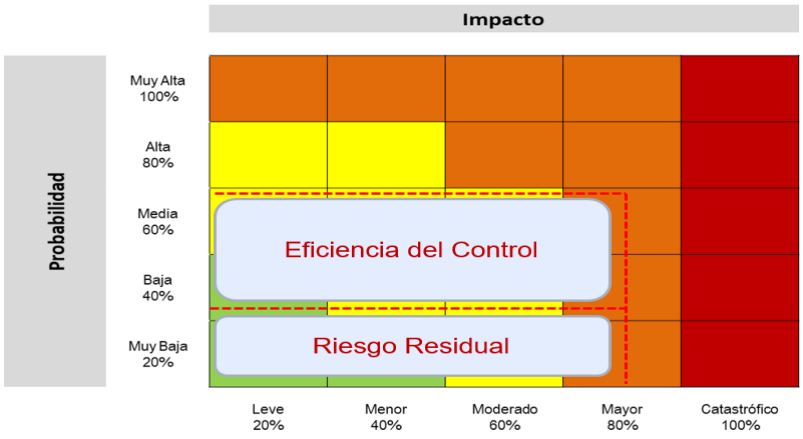
Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas V7, 2025

Teniendo que en cuenta que es a partir de los controles que se dará el movimiento en la matriz de calor por lo cual es necesario tener en cuenta que el **Nivel de riesgo (riesgo residual):** es el resultado de aplicar la efectividad de los controles al riesgo inherente.

Ejemplo: Probabilidad Residual= baja 26%
Impacto Residual= mayor 80%

Para este caso, si bien el riesgo se mantiene en zona alta, se bajó el nivel de probabilidad de ocurrencia del riesgo.

Tabla 11 Desplazamiento de la matriz a partir de Controles



Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas V7, 2025

5.7 Niveles de Aceptación del Riesgo

La decisión que se toma frente a un determinado nivel de riesgo será acorde con los riesgos residuales aprobados por los líderes de procesos, teniendo la cuenta la metodología de la Administración del Riesgo de la entidad.
Además, el Departamento Administrativo de la Función Pública (DAFP) establece que, para los **riesgos de gestión y fiscales**, cuando se defina la opción de tratamiento **"Reducir"**, se deberá formular un plan de acción. Para los **riesgos de integridad** no existe aceptación del riesgo, por lo que estos deberán conducir a la formulación de acciones para su tratamiento.

5.8 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

Nota: De acuerdo con el Acta N° 002 del Comité de Coordinación de Control Interno de la entidad, la identificación de los Riesgo de Seguridad de la Información estará Sujetos a la Socialización y Ejecución de los Planes del Decreto 612 del 2018 "*por la cual se fijan Directrices de los planes Institucionales y Estratégicos al Plan de Acciono r parte de las entidades del Estado" donde están relacionados los siguiente:*

10. Plan Estratégico de Tecnologías de la Información y las Comunicaciones –PETI,

11. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

12. Plan de Seguridad y Privacidad de la Información

Los cuales son documentos necesarios para lograr una identificación de los riesgos de Seguridad de la Información y crear el Procedimiento de Tecnologías de la Información

En concordancia con lo establecido en la Resolución N° 0092 del 30 de marzo del 2023 "*por medio de la cual se actualiza el procedimiento y la política de Administración del riesgo de la Corporación para el Desarrollo Sostenible del Norte y ele Oriente amazónico CDA y se deroga la Resolución 029 del 29 de enero del 2022"*, en su Artículo Quinto se dispone que, **"La identificación del riesgo por seguridad de la información estará sujeto a la socialización y ejecución del Plan Estratégico de Tecnologías de la Información y las Comunicaciones-PETI, Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información y Plan de Seguridad y Privacidad de la Información como elementos necesarios para la documentación del procedimiento de tecnologías de la información**".

5.9 Otras Disposiciones con relación a la Gestión de los Riesgos Tratamiento del Riesgo

Es la preparación e implementación de los planes de acción como herramienta para el tratamiento del riesgo, el cual parte, de establecer los responsables, las fechas de implementación, fecha se seguimiento, y el estado del riesgo (curso o finalizado) partiendo del trabajo que se realizan conjuntamente entre la Primera Línea de Defensa y la Tercera Línea de Defensa.

Tabla 12 Plan de Acción para el Tratamiento del Riesgo

Parte 3 Planes de acción (para la opción de tratamiento reducir):

Plan de Acción	Responsable	Fecha Implementación	Fecha Seguimiento	Seguimiento	Estado
Automatizar la lista de chequeo que utiliza el profesional de contratación, a fin de reducir la posibilidad de error humano y elevar la productividad del proceso.	Oficina de TIC	30/11/2020	30/06/2020	Se han adelantado las actividades de levantamiento de requerimientos funcionales para la automatización de la lista de chequeo.	En curso

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas V7, 2025

5.9.1 Acciones ante los Riesgos Materializados

Tabla 13 Acciones de respuesta al riesgo Materializado

Tipos de Riesgos	Responsable	Acción
	Líder de proceso	1. Informar a la oficina Asesora de planeación como Segunda Línea Defensa sobre el posible hecho encontrado y generar la alerta de una posible materialización del riesgo (Gestión, Integridad o fiscal).

Gestión, Integridad y Fiscal		**2.** Revisar los controles existentes y actualizar el mapa de riesgos. **3.** Dar cumplimiento a las acciones o recomendaciones emitidas por del Comité de Coordinación de Control Interno.
	Oficina Asesora de Control Interno	**1.** Convocar al Comité de Control de la entidad para informar sobre el hecho de la materialización de un riesgo (Gestión, Integridad o Fiscal) **2.** Realizar las respectivas recomendaciones ante el comité de control interno para la toma de decisiones. **3.** Verificar que se tomen las acciones y se actualice el mapa de riesgo correspondiente.
	Comité de control Interno	1. Dar las respectivas recomendaciones o acciones necesarias para corregir y prevenir que se vuelva a materializar el riesgo (Gestión, Integridad o Fiscal).

6 CONTROL DE CAMBIOS

CONTROL DE CAMBIOS	
FECHA	**NATURALEZA DEL CAMBIO**
27 de Marzo de 2017	Creación de la Política de Administración del Riesgo Resolución 106 del 27 de marzo del 2017.
29 de Noviembre de 2018	Se actualiza la Política de Administración de acuerdo con la Guía para la Gestión del Riesgo de Corrupción Versión 4 Diciembre 2014 Resolución 406 del 29 de noviembre 2018.
29 de Enero de 2021	Por la cual se adopta la Política de Administración del Riesgo en la Corporación para el Desarrollo Sostenible del Norte y el Oriente Amazónico CDA Resolución 029 de Enero del 2021
22 de Marzo de 2023	Se actualiza la Política de Administración de acuerdo a la Guía para la Administración del Riesgo y el Diseño de controles en entidades públicas Versión 6 Noviembre 2022. Se adopta bajo la Resolución 92 del 30 de marzo del 2023
28 de Febrero de 2025	Se actualiza la Política de Administración de Riesgos en base a la Actualización de la Política de Control Interno mediante Resolución N° 362 del 19 de Noviembre del 2024.
22 de Julio de 2026	Se actualiza la Política de Administración del Riesgo con el fin de incorporar los riesgos fiscales dentro de la gestión institucional, actualizar la denominación de riesgos de corrupción por riesgos de integridad y armonizar el documento con el procedimiento institucional de Administración de Riesgos de Gestión, Integridad, Fiscales y Oportunidades y los lineamientos vigentes del Departamento Administrativo de la Función Pública (DAFP).

Nota: De acuerdo con la Resolución N° 0092 del 30 de marzo del 2023 "*por medio de la cual se actualiza el procedimiento y la política de Administración del riesgo de la Corporación para el Desarrollo Sostenible del Norte y ele Oriente amazónico CDA y se deroga la Resolución 029 del 29 de enero del 2022",* en su artículo sexto se establece que, "Ordénese que la Política y procedimiento de administración de riesgos en la Corporación CDA, no requerirá para su actualización un nueva acta Administrativo, solo se actualizara el control de cambios del Anexo 1 el cual consta del 27 folios de la presente resolución, de acuerdo a los cambios normativos.