GUÍA PARA LA GESTIÓN DE RIESGOS Y OPORTUNIDADES

CORPORACIÓN AUTÓNOMA REGIONAL DEL ATLÁNTICO - C.R.A.

BARANQUILLA – ATLÁNTICO
2026

TABLA DE CONTENIDO

0. INTRODUCCIÓN 4
1. POLÍTICA DE GESTIÓN DEL RIESGO 4
2. TÉRMINOS Y DEFINICIONES 6
3. NIVELES DE RESPONSABILIDAD Y AUTORIDAD FRENTE A LA GESTIÓN DEL RIESGO 11
4. METODOLOGÍA PARA LA GESTIÓN DEL RIESGO 12
4.1. IDENTIFICACIÓN DEL RIESGO 12
4.2 DETERMINAR LA PROBABILIDAD 13
4.3 REGISTRO DE RIESGOS INSTITUCIONALES 13
4.3.1 ASIGNACIÓN DEL IMPACTO RIESGOS INSTITUCIONALES 14
4.4 GESTIÓN DE RIESGOS PARA LA INTEGRIDAD PÚBLICA 15
4.4.1 AMENAZAS PARA LA INTEGRIDAD PÚBLICA 16
4.4.2 SOBORNO 16
4.4.3 FRAUDE 17
4.4.4 INADECUADA GESTIÓN DEL CONFLICTO DE INTERESES 18
4.4.5 CORRUPCIÓN 19
4.4.6 LAVADO DE ACTIVOS, FINANCIACIÓN DEL TERRORISMO Y FINANCIACIÓN DE LA PROLIFERACIÓN DE ARMAS (LA/FT/FP) 20
4.5 REGISTRO DE RIESGOS DE INTEGRIDAD 21
4.5.1 ASIGNACIÓN DEL IMPACTO DE LOS RIESGOS DE INTEGRIDAD 22
4.6 REGISTRO DE RIESGOS FISCALES 22
4.6.1 ASIGNACIÓN DEL IMPACTO DE LOS RIESGOS FISCALES 26
4.7 REGISTRO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 26
4.7.1 ASIGNACIÓN DEL IMPACTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 31
4.8 ESTIMAR EL NIVEL DEL RIESGO INHERENTE 31
4.9 VALORACIÓN DEL RIESGO RESIDUAL 32

4.10 ACCIONES EN CASO DE MATERIALIZACIÓN DEL RIESGO 34
4.11 ARTICULACIÓN CON EL SISTEMA DE GESTIÓN INTEGRAL Y OTROS 35
5. TRATAMIENTO DE RIESGOS 36
6. METODOLOGÍA PARA LA GESTIÓN DE LAS OPORTUNIDADES 37
6.1 IDENTIFICACIÓN DE LA OPORTUNIDAD 38
6.2 VALORACIÓN DE LAS OPORTUNIDADES 39
6.3 ACTIVIDADES PARA LA GESTIÓN DE LAS OPORTUNIDADES 40
7. SEGUIMIENTO, ACTUALIZACIÓN Y VERIFICACIÓN DE LOS MAPAS DE RIESGO Y OPORTUNIDADES 41
7.1 SEGUIMIENTO DE LOS RIESGOS Y OPORTUNIDADES 41
7.2 ACTUALIZACIÓN Y VERIFICACIÓN DE LOS MAPAS DE RIESGO Y OPORTUNIDADES 42

0. INTRODUCCIÓN

El desarrollo de cualquier actividad está expuesto a situaciones que pueden impactar en forma negativa y afectar de cierta manera los objetivos propuestos. Como consecuencia de la diversidad de riesgos existentes, se requiere un acercamiento más profundo, metodológico y sistemático a la gestión de estos.

Por lo anterior y teniendo en cuenta que todas que todas las organizaciones independientemente de su tamaño y naturaleza están expuestas a diferentes riesgos o eventos que pueden poner en peligro su existencia, el gobierno nacional introduce en las entidades públicas el concepto de Administración y/o Gestión de Riesgos, el cual se define como "*Un 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*"[1].

La presente guía establece los lineamientos para identificar, valorar, tratar, monitorear y comunicar los riesgos institucionales, incorporando de manera transversal los riesgos de integridad conforme al Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP.

La incorporación del enfoque de integridad permitirá fortalecer la prevención de conductas contrarias a los principios de la función pública, tales como el abuso de poder, el conflicto de interés no gestionado, el favorecimiento indebido, el uso inapropiado de información, la manipulación de decisiones o cualquier actuación que comprometa el interés general.

1. POLÍTICA DE GESTIÓN DEL RIESGO

La Corporación Autónoma Regional del Atlántico – CRA está comprometida con la prevención, la legalidad, la transparencia, la ética pública y la integridad institucional. En cumplimiento del Decreto 1083 de 2015, gestiona de manera integral los riesgos que puedan afectar el cumplimiento de la ley, su misión y

[1] INTOSAI: Guía para las normas de control interno del sector público. http://www.intosai.org.

objetivos estratégicos, el uso eficiente y transparente de los recursos y la satisfacción de las partes interesadas.

Esta política aplica a todos los procesos de la entidad e incluye la identificación, valoración, tratamiento, monitoreo y seguimiento de los riesgos institucionales, de integridad, fiscales y de seguridad de la información, de conformidad a la metodología establecida en la Guía para la gestión integral del riesgo en entidades públicas, implementando controles preventivos, detectivos y correctivos, de acuerdo con la naturaleza y el nivel de exposición de los riesgos identificados.

La Alta Dirección define y promueve los lineamientos para la gestión integral del riesgo, fortaleciendo una cultura institucional basada en el mejoramiento continuo, la debida diligencia, el autocontrol, la transparencia, la integridad y la prevención de conductas contrarias a la ética y la legalidad. Asimismo, manifiesta su compromiso con la prevención, detección y mitigación del soborno, el fraude y los riesgos asociados al Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FP).

En el marco de esta política, la Corporación se compromete con la adopción de los siguientes lineamientos:

Antilavado de Activos, Contra la Financiación del Terrorismo y Contra la Financiación de la Proliferación de Armas de Destrucción Masiva (ALA/CFT/CFP)

La Corporación manifiesta su compromiso con el fortalecimiento de una cultura institucional orientada a la prevención, detección y mitigación de los riesgos asociados al Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FP). Asimismo, promueve el reporte oportuno de cualquier operación, conducta o situación que corresponda a las señales de alerta definidas por la entidad, garantizando la confidencialidad y la protección de quienes realicen dichos reportes, sin temor a represalias.

Antisoborno

La Corporación manifiesta su compromiso con el fortalecimiento de una cultura institucional orientada a la prevención, detección y mitigación del soborno, promoviendo la integridad, la transparencia y el cumplimiento de los principios éticos en el desarrollo de sus actividades. Asimismo, fomenta el reporte oportuno de cualquier conducta, intento de soborno o situación que corresponda a las señales

de alerta definidas por la entidad, garantizando la confidencialidad y la protección de quienes realicen dichos reportes, sin temor a represalias.

Antifraude

La Corporación manifiesta su compromiso con el fortalecimiento de una cultura institucional orientada a la prevención, detección, gestión y mitigación del fraude. Asimismo, promueve el reporte oportuno de cualquier acto, intento o sospecha de fraude, garantizando la confidencialidad y la protección frente a represalias de quienes realicen dichos reportes, así como el estricto cumplimiento de la normativa y los lineamientos institucionales en materia de prevención y control del fraude.

La Secretaría General, a través de la Coordinación del Sistema de Gestión Integrado y con el apoyo de la Oficina de Control Interno, liderará y coordinará las acciones relacionadas con la implementación y seguimiento de esta política, promoviendo la aplicación de controles, el monitoreo de los riesgos y las alertas identificadas, la socialización de responsabilidades y la formulación e implementación de acciones de mejora.

2. TÉRMINOS Y DEFINICIONES[2]

Para los efectos de la presente Política, es importante tener en cuenta los siguientes términos y definiciones:

1) Abuso de poder: utilización de la autoridad, posición o funciones para obtener beneficios privados, dirigir decisiones de forma indebida o afectar el principio de imparcialidad.

2) Activo de la información: Cualquier elemento que tiene valor para una organización y que contiene, procesa o soporta información, por lo que debe ser protegido.

3) ALA/CFT/CFP: Antilavado de Activos, Contra la Financiación del Terrorismo y Contra la Financiación de la Proliferación de Armas de Destrucción Masiva.

4) Gestión de Riesgos: Conjunto de elementos de control que, al interrelacionarse, permiten a la entidad pública evaluar aquellos eventos negativos, tanto internos

[2] Guía para la Gestión Integral del Riesgo en Entidades Públicas. Departamento Administrativo de la Función Pública (DAFP).

como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos que permitan identificar oportunidades para un mejor cumplimiento de su función. Se constituye en el componente de control que al interactuar sus diferentes elementos le permite a la entidad pública autocontrolar aquellos eventos que pueden afectar el cumplimiento de sus objetivos.

5) Apetito de riesgo: Es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

6) Análisis de riesgo: Elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la corporación para su aceptación y manejo. Se debe llevar a cabo un uso sistemático de la información disponible para determinar qué tan frecuentemente pueden ocurrir eventos especificados y la magnitud de sus consecuencias.

7) Capacidad de riesgo: es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad.

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

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

10) Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

11) Conflicto de interés: situación en la que el interés particular de un servidor público, contratista o colaborador puede influir, interferir o percibirse como influyente en el ejercicio imparcial de sus funciones o responsabilidades.

12) Consecuencia: Efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

13) Contexto: Definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo. A partir de los factores que se definan es posible establecer las causas de los riesgos a identificar.

14) Contexto externo: Se determinan las características o aspectos esenciales del entorno en el cual opera la entidad.

15) Contexto interno: Se determinan las características o aspectos esenciales del ambiente en el cual la organización busca alcanzar sus objetivos.

16) Control: Medida que permite reducir o mitigar un riesgo.

17) Corrupción: Todo acto que implique desviación de la gestión administrativa o de los recursos públicos y privados para obtener un beneficio propio o para un tercero.

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

19) Evaluación del control: Elemento de control que, basado en un conjunto de mecanismos de verificación y evaluación, determina la calidad y efectividad de los controles internos a nivel de los procesos y de cada área organizacional responsable, permitiendo emprender las acciones de mejoramiento del control requeridas. Se basa en una revisión periódica y sistemática de los procesos de la entidad para asegurar que los controles establecidos son aún eficaces y apropiados.

20) Evaluación del riesgo: Proceso utilizado para determinar las prioridades de la Administración del Riesgo comparando el nivel de un determinado riesgo con respecto a un estándar determinado.

21) Evento: Incidente o situación que ocurre en un lugar determinado durante un período de tiempo determinado. Este puede ser cierto o incierto y su ocurrencia puede ser única o ser parte de una serie.

22) Fraude: Errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros.

23) Frecuencia: Número de veces al año en el cual se realiza la actividad que conlleva al riesgo.

24) Gestión del riesgo fiscal: Son las actividades que debe desarrollar cada Entidad y todos los gestores públicos para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial)

25) Identificación del riesgo: Elemento de control, que posibilita conocer los eventos potenciales, estén o no bajo el control de la entidad pública, que ponen en riesgo el logro de su misión, estableciendo los agentes generadores, las causas y los efectos de su ocurrencia. Se puede entender como el proceso que permite determinar qué podría suceder, por qué sucedería y de qué manera se llevaría a cabo.

26) Impacto: Consecuencias o daños que puede ocasionar a la corporación la materialización del riesgo, expresado cualitativa o cuantitativamente, siendo una pérdida, lesión, desventaja o ganancia. Puede haber un rango de posibles resultados asociados con un evento.

27) Integridad pública: actuación consistente con los valores, principios y deberes de la función pública, orientada al interés general, a la legalidad, a la transparencia y al uso adecuado de los recursos públicos.

28) Monitorear: Comprobar, Supervisar, observar, o registrar la forma en que se lleva a cabo una actividad con el fin de identificar sus posibles cambios.

29) Nivel de riesgo: es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

30) Pérdida: Consecuencia negativa que trae consigo un evento.

31) Probabilidad: Grado en el cual es probable que ocurra de un evento, este se debe medir a través de la relación entre los hechos ocurridos realmente y la cantidad de eventos que pudieron ocurrir.

32) Proceso de administración de riesgo: Aplicación sistemática de políticas, procedimientos y prácticas de administración a las diferentes etapas de la administración del riesgo.

33) Punto de riesgo: Actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública.

34) Reducción del riesgo: Aplicación de controles para reducir las probabilidades de ocurrencia de un evento y/o su ocurrencia.

35) Riesgo: Posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

36) 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.

37) Riesgo de integridad: Posibilidad de que, por acción, omisión o tolerancia, se presenten conductas o situaciones que afecten la ética pública, la transparencia, la imparcialidad, la legalidad, la confianza ciudadana o el cumplimiento de los fines institucionales.

38) 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).

39) Riesgo inherente: Es aquel al que se enfrenta la corporación en ausencia de acciones o controles para modificar su probabilidad o impacto.

40) Riesgo residual: Nivel de riesgo que permanece luego de tomar medidas de tratamiento de riesgo o aplicación de los controles.

41) Soborno: Ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar.

42) 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.

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

3. NIVELES DE RESPONSABILIDAD Y AUTORIDAD FRENTE A LA GESTIÓN DEL RIESGO

La Corporación Autónoma Regional del Atlántico, en concordancia con el Modelo Integrado de Planeación y Gestión MIPG adoptado por la Resolución 0000038 de 2024, establece la operatividad de la gestión del riesgo basado en las líneas de defensa requerido por la *Guía para la gestión integral del riesgo en entidades públicas* en su versión vigente.

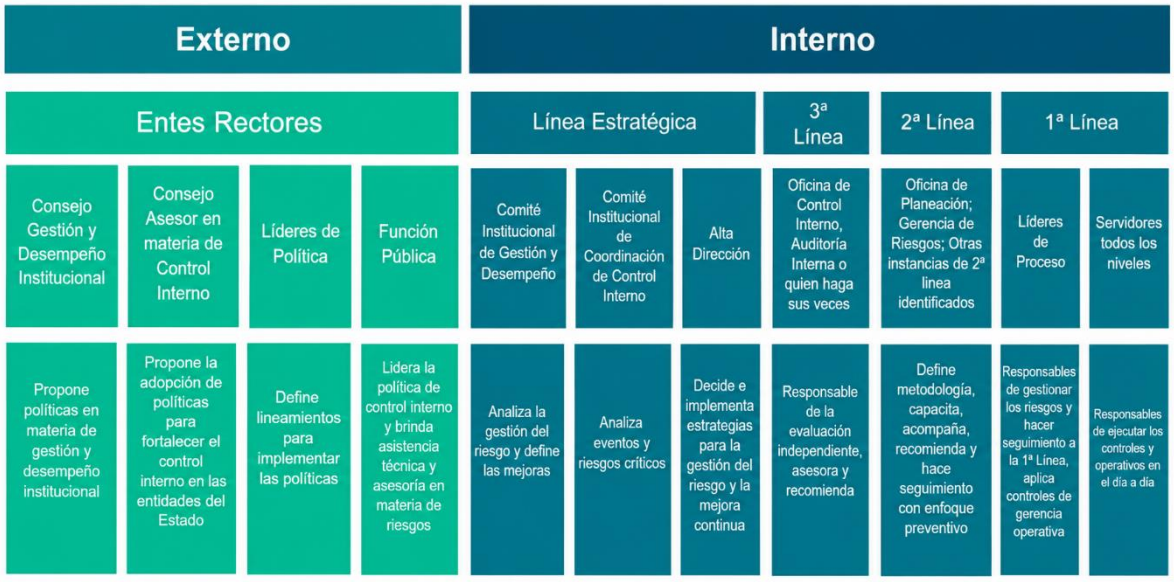


Figura No.1 Operatividad Institucional para la administración del riesgo.
Fuente: *Dirección de Gestión y Desempeño Institucional de Función Pública, 2025.*

El establecimiento de las responsabilidades y autoridades frente a la gestión del riesgo se registran en la *Guía de roles, responsabilidades y autoridades en el Sistema de Gestión Integral* en su versión vigente.

La gestión de riesgos de integridad se articulará con los mecanismos institucionales de control interno, la gestión documental, la transparencia, el control disciplinario interno y el manual de buen gobierno de la corporación.

4. METODOLOGÍA PARA LA GESTIÓN DEL RIESGO

Para determinar la metodología para la gestión del riesgo adoptada por la corporación, se toma como referencia la establecida por el Departamento Administrativo de la Función Pública, la cual estipula una serie de etapas que se deben desarrollar para realizar una adecuada gestión del riesgo. Para facilitar su aplicación, la corporación ha diseñado una herramienta (mapa de riesgos y oportunidades) que permite realizar la identificación, valoración, el monitoreo y seguimiento a los riesgos.

4.1. IDENTIFICACIÓN DEL RIESGO

En esta etapa se deben establecer los riesgos y su tipología, las fuentes generadoras de riesgos, sus causas y sus consecuencias.

Para el análisis, los responsables de los procesos junto con su equipo de trabajo realizan la identificación de los riesgos que puedan afectar el desempeño de los procesos considerando:

- El contexto interno y externo (Ver documento *Análisis del Contexto Interno y Externo de la Organización*).
- Las necesidades y expectativas de las partes interesadas (Ver documento *Análisis de partes interesadas*)
- Cuestiones o situaciones de riesgos que afecten el cumplimiento de sus funciones y objetivos institucionales trazados en las líneas estratégicas.

El mapa de riesgos y oportunidades será el instrumento con el que contarán los procesos para la identificación de los siguientes riesgos:

- Riesgos institucionales.
- Riesgos de integridad.
- Riesgos fiscales.
- Riesgos de seguridad de la información.

Una vez identificados los riesgos, es preciso registrar dentro del formato *Mapa de riesgos y oportunidades* la descripción de cada evento inductor (Riesgo), fuentes, causas y sus consecuencias potenciales en su estado natural, es decir, sin considerar medidas de mitigación. De esta forma se determina aquéllos que, en caso de ocurrir, pueden significar una pérdida o daño. Estos aspectos se registran en las primeras columnas de la estructura del mapa de riesgos y oportunidades adoptado en la Corporación.

4.2 DETERMINAR LA PROBABILIDAD

Se entiende por Probabilidad, la posibilidad de ocurrencia del riesgo y estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

Bajo el criterio de probabilidad, el líder del proceso debe medir el riesgo tomando como referencia las siguientes especificaciones registradas en la tabla 1.

Nivel	Probabilidad	Frecuencia de la Actividad
1	Muy Baja – 20%	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año
2	Baja – 40%	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año
3	Media – 60%	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año
4	Alta – 80%	La actividad que conlleva el riesgo se ejecuta más de 500 veces al año y máximo 5000 veces por año
5	Muy Alta – 100%	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año

Tabla No. 1 Criterios para definir el nivel de probabilidad

Frecuencia: Este campo corresponde al número de veces al año en el cual se realiza la actividad que conlleva al riesgo.

Nota: El análisis de probabilidad deberá ajustarse dependiendo del proceso y de la disponibilidad de datos históricos sobre al evento o riesgo identificado. En caso de no contar con datos históricos, se trabajará de acuerdo con la experiencia de los funcionarios que desarrollan el proceso y de sus factores internos y externos.

4.3 REGISTRO DE RIESGOS INSTITUCIONALES

El registro de los riesgos institucionales se debe realizar en la sección del *mapa de riesgos y oportunidades* que se muestra en la figura No.2

Código del riesgo	IDENTIFICACIÓN DE RIESGOS INSTITUCIONALES				ANÁLISIS DE RIESGO INHERENTE			
	Riesgo	Fuente	Causas	Consecuencias Potenciales	Impacto		Probabilidad	Riesgo Inherente (ZIR)
					Afectación económica	Afectación reputacional	Número de veces que se realiza la actividad	
					1	1	1	Zona de Riesgo Baja

Figura No. 2 Espacio del mapa de riesgos y oportunidades destinado para el diligenciamiento de los riesgos institucionales

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la organización, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

En lo relativo a las fuentes que inducen los riesgos tienen las siguientes:

- Procesos.
- Talento Humano.
- Tecnología.
- Infraestructura.
- Eventos externos.

4.3.1 ASIGNACIÓN DEL IMPACTO RIESGOS INSTITUCIONALES

Por impacto se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Para la elaboración de la tabla de criterios se establecen como variables principales la afectación económica y reputacional.

Para su determinación se utiliza la tabla 2, la cual registra los criterios para definir el nivel de impacto.

Para determinar el nivel del impacto, el líder del proceso identificará y seleccionará el rango que refleja la consecuencia de la activación del inductor de riesgo. Cuando se presenten ambos impactos para un riesgo (económico y reputacional) con diferentes niveles, se deberá tomar el nivel más alto, así, por ejemplo: para un riesgo identificado se define un impacto económico en nivel mayor e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel mayor.

Nivel	% de Impacto	Afectación Económica	Afectación Reputacional
1	Leve - 20%	Afectación menor a 1 SMLMV	El riesgo afecta la imagen de algún área de la entidad.
2	Menor - 40%	Entre 1 y 5 SMLMV	El riesgo afecta la imagen de la entidad a nivel interno, de conocimiento general, de junta directiva y accionistas y/o de proveedores.
3	Moderado -60%	Entre 5 y 10 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
4	Mayor - 80%	Entre 10 y 100 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
5	Catastrófico - 100%	Mayor a 100 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

Tabla No. 2 Criterios para definir el nivel de impacto

4.4 GESTIÓN DE RIESGOS PARA LA INTEGRIDAD PÚBLICA

En concordancia con la Guía para la Gestión Integral del Riesgo en Entidades Públicas en su versión vigente, la Corporación Autónoma Regional del Atlántico incorpora la Gestión de Riesgos para la Integridad Pública como desarrollo específico y diferenciado de los riesgos que pueden afectar la transparencia y legalidad en el ejercicio de la función pública, en articulación con la Política de Gestión de Riesgos de la Corporación.

4.4.1 AMENAZAS PARA LA INTEGRIDAD PÚBLICA

Con el fin de identificar y valorar los riesgos de integridad, la Corporación reconoce las principales amenazas que pueden afectar la integridad pública. Para cada una de ellas se describen sus manifestaciones más comunes, los procesos o actividades potencialmente expuestas y los controles sugeridos para prevenir, mitigar y gestionar dichos riesgos.

La gestión de riesgos de integridad se desarrollará mediante las etapas generales establecidas en la presente guía (identificación, análisis, valoración, tratamiento, monitoreo), aplicando criterios específicos para reconocer:

- Alto grado de discrecionalidad en la toma de decisiones.
- Contacto directo con usuarios, proveedores o contratistas.
- Administración, asignación o disposición de recursos públicos.
- Acceso a información reservada, privilegiada o sensible.
- Expedición de permisos, autorizaciones, conceptos o licencias.
- Ejercicio de autoridad ambiental.
- Realización de visitas de inspección, vigilancia y control.
- Desarrollo de procesos sancionatorios.
- Elaboración de estudios técnicos.
- Contratación y supervisión contractual.
- Ausencia o debilidad de trazabilidad en las decisiones.

4.4.2 SOBORNO

El soborno se entiende como el ofrecimiento, promesa, entrega, aceptación o solicitud de un beneficio indebido para influir en el ejercicio de la función pública.

El listado a continuación presenta procesos o actividades potencialmente expuesto al riesgo de soborno. El listado tiene carácter orientador, por lo tanto, no es exhaustivo.

Posibles manifestaciones	Procesos o actividades potencialmente expuestos	Controles sugeridos
Pagos o dádivas a cambio de agilizar trámites, favorecer proponentes o evitar sanciones	Adquisición de bienes y servicios Manejo, control y seguimiento ambiental	Operación del Código de Integridad Lineamientos sobre regalos, atenciones, hospitalidades y beneficios

Ofrecimiento o aceptación de dinero Regalos, atenciones o invitaciones indebidas Promesas de vinculación laboral o contractual Favores personales Beneficios para familiares o personas relacionadas Donaciones o patrocinios utilizados para influir en una decisión Intermediación de terceros para ofrecer o entregar una ventaja indebida Solicitud de beneficios para agilizar, omitir o modificar una actuación administrativa		Declaraciones de ausencia de ofrecimientos indebidos en actividades críticas Acompañamiento en visitas sensibles Trazabilidad de decisiones y actuaciones Supervisión selectiva de trámites de alto riesgo Revisión de casos con modificaciones, excepciones o tiempos atípicos Operación de canales de denuncia y protección frente a represalias

4.4.3 FRAUDE

El fraude se entiende como acto u omisión intencional mediante el cual se engaña, oculta, altera, falsifica o presenta información incorrecta con el propósito de obtener un beneficio indebido para sí o para un tercero, o de causar un perjuicio a la entidad, al patrimonio público o a otras partes interesadas. Los errores involuntarios deberán gestionarse como fallas operativas, incumplimientos o riesgos institucionales, salvo que existan evidencias de intencionalidad.

Posibles manifestaciones	**Procesos o actividades potencialmente expuestos**	**Controles sugeridos**
Adulteración de soportes documentales Doble facturación Apropiación de recursos	Gestión Financiera Adquisición de Bienes y Servicios Gestión Documental y Archivo Gestión del Talento Humano	Segregación de funciones Conciliaciones periódicas Trazabilidad documental y auditorías

Alteración de informes técnicos o resultados de visitas Falsificación de firmas, registros o evidencias Manipulación de criterios de evaluación Certificación de actividades no realizadas Ocultamiento o eliminación de documentos Alteración de información en sistemas institucionales Suplantación de identidad Reconocimiento de pagos o beneficios sin cumplimiento de requisitos Presentación de información falsa por proveedores, contratistas, usuarios o servidores Manipulación de indicadores o reportes de gestión	Gestión de Tecnología de la Información Gestión de Proyectos Ambientales Manejo, Control y Seguimiento Ambiental Soporte Jurídico Planificación para el Desarrollo Sostenible Gestión de la Infraestructura	

4.4.4 INADECUADA GESTIÓN DEL CONFLICTO DE INTERESES

El conflicto de interés se entiende como la situación en la que el interés particular de un servidor público, contratista, supervisor, interventor, miembro de comité o colaborador puede influir, interferir o percibirse como influyente en el ejercicio imparcial de sus funciones o responsabilidades.

El conflicto puede ser real, potencial o aparente.

Su existencia no implica automáticamente una conducta irregular; el riesgo surge cuando no se declara, no se analiza o no se gestiona adecuadamente.

Posibles manifestaciones	Procesos o actividades potencialmente expuestos	Controles sugeridos
Participación en decisiones, contratación o supervisión donde existe un interés personal, familiar o económico no declarado	Gestión Financiera Adquisición de Bienes y Servicios Manejo, Control y Seguimiento Ambiental	Declaración inicial, periódica y sobreviniente de conflictos de intereses Procedimiento para recibir, analizar y resolver declaraciones Registro de conflictos declarados y decisiones adoptadas Reasignación formal de asuntos cuando corresponda Documentación de impedimentos y recusaciones Declaraciones específicas para integrantes de comités evaluadores Verificación de relaciones personales, familiares, económicas o profesionales relevantes Seguimiento al cumplimiento de las medidas de manejo Conservación de evidencias con las restricciones de confidencialidad aplicables

4.4.5 CORRUPCIÓN

La corrupción se entiende como el uso del poder o de los recursos públicos, por acción u omisión, para obtener un beneficio propio o para un tercero, en detrimento del interés general.

Posibles manifestaciones	Procesos o actividades potencialmente expuestos	Controles sugeridos
Direccionamiento de procesos de selección, tráfico de influencias, apropiación o desviación de recursos públicos	Adquisición de Bienes y Servicios Gestión Financiera Manejo, Control y Seguimiento Ambiental Soporte Jurídico Gestión del Talento Humano Gestión de Proyectos Ambientales Gestión de la Infraestructura Planificación para el Desarrollo Sostenible	Segregación de funciones Publicidad de actuaciones y decisiones Trazabilidad de modificaciones y aprobaciones Verificación independiente de requisitos Criterios objetivos documentados Analítica de datos para detectar operaciones atípicas Auditorías focalizadas Canales de denuncia Seguimiento a señales de alerta Control de accesos a sistemas e información

4.4.6 LAVADO DE ACTIVOS, FINANCIACIÓN DEL TERRORISMO Y FINANCIACIÓN DE LA PROLIFERACIÓN DE ARMAS (LA/FT/FP)

La Corporación reconoce la necesidad de identificar, prevenir, controlar y mitigar los riesgos asociados al lavado de activos, la financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva (LA/FT/FP), mediante la adopción de medidas orientadas a fortalecer la transparencia, la legalidad y la debida diligencia en sus procesos institucionales, con el fin de prevenir que sus recursos, operaciones, contratos, convenios, trámites o relaciones con terceros puedan ser utilizados, de manera directa o indirecta, para ocultar el origen ilícito de activos, facilitar la canalización de recursos hacia actividades terroristas o contribuir a la financiación de la proliferación de armas de destrucción masiva.

Posibles manifestaciones	Procesos o actividades potencialmente expuestos	Controles sugeridos
Pagos o contratos con contrapartes de origen o destino no justificado, fraccionamiento de operaciones, relaciones con terceros en listas restrictivas o de alto riesgo	Gestión Financiera Adquisición de Bienes y Servicios Manejo, Control y Seguimiento Ambiental	Debida diligencia de contrapartes según nivel de riesgo Monitoreo de operaciones inusuales Reporte de operaciones sospechosas a la UIAF – Unidad de Información y Análisis Financiero y demás autoridades competentes

La gestión de estos riesgos encontrará sus principales lineamientos en el capítulo x. Manual de Debida Diligencia, que hace parte del Manual de Buen Gobierno de la corporación.

4.5 REGISTRO DE RIESGOS DE INTEGRIDAD

El registro de los riesgos de integridad se debe realizar en la sección del *mapa de riesgos y oportunidades* que se muestra en la figura No.3.

Código del riesgo	IDENTIFICACIÓN DE RIESGOS DE INTEGRIDAD				ANÁLISIS DE RIESGO INHERENTE			
	Riesgo	Fuente	Causas	Consecuencias Potenciales	Impacto		Probabilidad	Riesgo Inherente (ZIR)
					Afectación económica	Afectación reputacional	Número de veces que se realiza la actividad	
					1	1	1	Zona de Riesgo Baja

Figura No. 3 Espacio del mapa de riesgo y oportunidades destinado para el diligenciamiento de los riesgos de integridad

El registro de los riesgos de integridad se realiza de manera similar a los riesgos institucionales en los campos de *riesgo, fuente, causas y consecuencias potenciales,* sin embargo, se cuenta con una variación para la determinación del impacto debido a la sensibilidad de este tipo de riesgos.

Para la redacción de los riesgos de integridad pública se tendrán en cuenta los lineamientos establecidos en la *Guía para la Gestión Integral del Riesgo en Entidades Públicas*, en su numeral 6.3.5.1. Identificación y valoración de riesgos para la integridad pública en la Política para la Gestión Integral de Riesgos.

4.5.1 ASIGNACIÓN DEL IMPACTO DE LOS RIESGOS DE INTEGRIDAD

Para los riesgos de integridad, el análisis de impacto se realizará teniendo en cuenta solamente los niveles ***moderado***, ***mayor*** *y* ***catastrófico*** listados en la tabla 2. Criterios para definir el nivel de impacto, dado que estos riesgos siempre serán significativos.

Lo anterior, debido a que su materialización puede afectar la legalidad, la ética pública, la imparcialidad, la transparencia, la confianza ciudadana y la legitimidad institucional.

4.6 REGISTRO DE RIESGOS FISCALES

El registro de los riesgos fiscales se debe realizar en la sección del *mapa de riesgos y oportunidades* que se muestra en la figura No.4.

Código del riesgo	IDENTIFICACIÓN DE RIESGOS FISCALES		ANÁLISIS DE RIESGO INHERENTE			
	Punto de riesgo fiscal	Circunstancias inmediatas	Impacto		Probabilidad	Riesgo Inherente (ZIR)
			Afectación económica	Afectación reputacional	Número de veces que se realiza la actividad	
			1	1	1	Zona de Riesgo Baja

Figura No. 4 Espacio del mapa de riesgos y oportunidades destinado para el diligenciamiento de los riesgos fiscales

En el registro de los riesgos fiscales se deben considerar los conceptos de *Punto de riesgo fiscal* y *Circunstancias inmediatas* establecidos por la *Guía para la Gestión Integral del Riesgo en Entidades Públicas* publicada por el Departamento Administrativo de Función Pública *DAFP,* por lo tanto, la Corporación Autónoma Regional del Atlántico adopta el listado enunciativo de puntos de riesgo fiscal y causas inmediatas propuesto por el DAFP necesarios para la gestión de este tipo de riesgos, tal como se muestra en la tabla 3.

De igual forma como los demás riesgos, los riesgos institucionales deben recibir la asignación del nivel de probabilidad de acuerdo con la tabla No.1 del numeral 4.1.1 del presente documento.

Id Referencia	**Puntos de Riesgo Fiscal**	**Circunstancia Inmediata**
	Actividad en la que potencialmente se origina el riesgo fiscal	*Situación **por la que** se presenta el riesgo*
1	Cumplimiento de las normas y obligaciones ante autoridades	Pago de multas, cláusulas penales o cualquier tipo de sanción
2	Cumplimiento de obligaciones	Pago de Intereses moratorios
3	Desplazamientos de los funcionarios y de los contratistas a lugares diferentes al domicilio de la entidad.	Pago de viáticos, honorarios o gastos de desplazamiento sin justificación o por encima de los valores establecidos normativamente
4	Liquidación de impuestos	Mayor valor pagado por concepto de impuestos
5	Operaciones, actas o actos en los que se reconocen saldos a favor de la entidad	Saldos o recursos a favor no cobrados
6	Custodiar de los bienes muebles de la entidad	Pérdida, extravío, hurto, robo o declaratoria de bienes faltantes pertenecientes a la Entidad
7	Avalúos a bienes inmuebles de la entidad	Error en los avalúos, afectando el valor de venta y/o negociación de un bien público
8	Custodiar de los bienes muebles de la entidad	Daño en bienes muebles de propiedad de la entidad
9	Suscripción de contratos cuyo objeto es o incluye la representación judicial o extrajudicial de la entidad	Valor pagado por concepto de honorarios de apoderado cuando ocurre vencimiento de términos en los procesos judiciales o cualquier otra omisión del apoderado
10	Pago de sentencias y conciliaciones	Intereses moratorios por pago tardío de sentencias y conciliaciones

11	Instrucción del Comité de Conciliación para iniciar acción de repetición	Caducidad de la acción de repetición o falencias en el ejercicio de esta acción, generando la imposibilidad de recuperar los recursos pagados por el Estado
12	Informe que acredite o anuncie la existencia de perjuicios generados a la entidad	Omisión en la obligación de impulsar acción judicial para cobrar clausula penal u otros perjuicios
13	Contratación de bienes o servicios	Contratación de bienes y servicios no relacionados con las funciones de la Entidad y que no generan utilidad
14	Contratación de bienes	Compra o inversión en bienes innecesarios o suntuosos
15	Contratación de estudios y diseños	Estudios y diseños recibidos y pagados y que no cumplen condiciones de calidad
16	Suscripción de contratos de estudios y diseños	Estudios y diseños con amparo de calidad vencido al momento de contratar la obra y/o al momento de la ocurrencia
17	Suscripción de contratos	Sobrecostos en precios contractuales
18	Suscripción de contratos	Pagos efectuados a causa de riesgos previsibles que debieron ser asignados al contratista en la matriz de riesgos previsibles y no se le asignaron
19	Suscripción de contratos	No incluir en el contrato de seguros - amparo de bienes de la entidad- todos los bienes muebles e inmuebles de la entidad
20	Suscripción de contratos	No exigir garantía única de cumplimiento contractual
21	Suscripción de contratos respecto de los cuales la ley establece un cubrimiento mínimo en los amparos de la garantía única de cumplimiento	Exigir garantía única de cumplimiento contractual con un cubrimiento inferior al exigido por la ley
22	Pagos efectuados a contratistas	Pagar bienes, servicios u obras a pesar de no cumplir las condiciones de calidad.
23	Constancias de recibo a satisfacción de bienes, servicios u obras, firmadas por supervisor o interventor	Bienes, servicios u obras inconclusos, no funcionales y/o que no brindan utilidad o beneficio
24	Modificaciones contractuales firmadas	Modificaciones contractuales cuyas causas son imputables al contratista total o parcialmente y cuyos costos colaterales asume la Entidad contratante
25	Giros efectuados por concepto de anticipo contractual	Mal manejo o fallas en la legalización de anticipos, no amortización del anticipo
26	Giros efectuados por concepto de anticipo contractual	Rendimientos financieros de recursos de anticipo o de cualquier recurso público no devueltos al tesoro público

27	Reconocimiento y pago de desequilibrio contractual	Reconocimiento y pago de desequilibrio contractual por causa imputable a la Entidad
28	Firma de actas contractuales de recibo parcial o final	Errores o imprecisiones en las actas de recibo parcial o final
29	Firma de adiciones de ítems, actividades o productos no previstos (contratos adicionales)	Adición de ítem, actividad o producto no previsto sin estudio de mercado y/o con sobrecosto
30	Firma de adiciones de ítems, actividades o productos inicialmente previstos (adiciones)	Mayores cantidades reconocidas y pagadas con valores unitarios superiores al pactado en el contrato
31	Actos administrativos sancionatorios contractuales emitidos y ejecutoriados	Cuantificación errada de multa o clausula penal
32	Obras recibidas a satisfacción	Colapso o fallas en la estabilidad de la obra
33	Pagos finales efectuados a contratistas	Ejecución de un alcance inferior al contratado y pago total del contrato
34	Actas de recibo final a satisfacción firmadas	Infuncionalidad de lo ejecutado
35	Contratos finalizados	Bienes, servicios u obras inconclusas y/o que no brindan utilidad o beneficio
36	Pagos efectuados a contratistas	Inadecuada deducción de impuestos, tasas o contribuciones al contratista
37	Pagos por concepto de comisión a éxito	Pago de comisiones a éxito sin debida justificación
38	Actas de liquidación suscritas	Suscripción de acta de liquidación con imprecisiones de fondo
39	Actas de liquidación suscritas	Suscripción de acta de liquidación sin relacionar las sanciones impuestas al contratista
40	Contratos finalizados en los que se contemplaba o requería liquidación.	Pérdida de competencia para liquidar por vencimiento del plazo legal, con saldos a favor de la Entidad
41	Actas de liquidación suscritas	Liquidación de mutuo acuerdo con recibo a satisfacción, habiendo imprecisiones o falsedades
42	Bienes u obras recibidas a satisfacción	Deterioro del bien u obra por indebido mantenimiento
43	Actas de recibo final a satisfacción firmadas	Suscripción de acta de recibo final con imprecisiones de fondo
43	Reintegro de saldos a favor de la entidad o pagos por parte de deudores	Reintegro de saldos a favor de la entidad sin indexación (reintegro sin actualización del dinero en el tiempo)
44	Predios adquiridos	Adquisición de predios sin las especificaciones técnicas requeridas

45	Pérdida de tenencia de bienes de la entidad	Pérdida de la tenencia de bienes inmuebles de la Entidad
46	Pago de subsidios, transferencias o beneficios a particulares	Bases de datos con falencias de información que genera pagos de subsidios u otros beneficios sin el cumplimiento de requisitos y condiciones
47	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidio u otros beneficios a personas fallecidas
48	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios u otros beneficios a personas que no tienen derecho a los mismos a la luz de requisitos de ley
49	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios por encima del beneficio otorgado
50	Deudas a favor de la entidad	Vencimiento de plazos para la labor de cobro directo (persuasivo o coactivo) o judicial

Tabla No. 3. Anexo 3. Catálogo indicativo de puntos de riesgo fiscal de la Guía para la Gestión Integral del Riesgo en Entidades Públicas, 2025.

4.6.1 ASIGNACIÓN DEL IMPACTO DE LOS RIESGOS FISCALES

Entendiendo la naturaleza de los riesgos fiscales, la asignación del nivel de impacto de este tipo de riesgos se debe realiza teniendo en cuenta los criterios establecidos por la tabla 2.

4.7 REGISTRO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La identificación y registro de los riesgos de seguridad de la información encuentra sus bases en el *Capítulo 5 Riesgos de Seguridad de la Información* de la Guía para la Gestión Integral del Riesgo en Entidades Públicas, y en la norma ISO 27001 en su versión vigente, en donde se identifican los siguientes tres (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que

podrían causar su materialización. A continuación, se mencionan un listado de amenazas y vulnerabilidades que podrían materializar los tres (3) riesgos previamente mencionados:

TIPO	AMENAZAS	ORIGEN
Daños físicos	Fuego	A, D, E
	Daños por el agua	A, D, E
	Contaminación	A, D, E
	Accidente grave	A, D, E
	Destrucción de equipos o medios	A, D, E
	Polvo, corrosión, congelación	A, D, E
Eventos naturales	Fenómeno climático	E
	Fenómeno sísmico	E
	Fenómeno volcánico	E
	Fenómeno meteorológico	E
	Inundación	E
Pérdida de servicios esenciales	Fallo del sistema de aire acondicionado	A, D
	Pérdida del suministro de energía	A, D, E
	Fallo del equipo de telecomunicaciones	A, D
Perturbación por radiación	Radiación electromagnética	A, D, E
	Radiación térmica	A, D, E
	Pulsos electromagnéticos	A, D, E
Compromiso de la información	Interceptación de señales de interferencia comprometedoras	D
	Espionaje remoto	D
	Intercepción furtiva	D
	Hurto de medios de comunicación o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	D
	Datos de fuentes no fiables	A, D
	Manipulación del hardware	D
	Manipulación del software	A, D
	Detección de posición	D
Fallas técnicas	Fallo del equipo	A
	Saturación del sistema de información	A, D
	Mal funcionamiento del software	A
	Incumplimiento en el mantenimiento de los sistemas de información	A, D
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta de programas informáticos	D
	Uso de programas informáticos o copiados	A, D
	Corrupción de datos	D
	Procesamiento ilegal de datos	D
Compromiso de funciones	Error en el uso	A
	Abuso de derechos	A, D

	Falsificación de derechos	D
	Negación de acciones	D
	Valoración de la disponibilidad de personal	A, D, E
Humano	Piratería informática	D
	Crímenes de la computación (destrucción o divulgación ilegal de información)	D
	Terrorismo (Ataques *DDoS*, penetración al sistema)	D
	Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	D
	Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos	D

Deliberadas (D), Fortuito (F) o Ambientales (A)

Tabla No. 4 Listado indicativo de amenazas que representa situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos. Fuente: ISO 27005:2022

TIPO	VULNERABILIDADES
Hardware	Mantenimiento insuficiente
	Instalación defectuosa de los medios de almacenamiento
	Falta de planes de sustitución periódica
	Susceptibilidad a la humedad, al polvo, a la suciedad
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura
	Almacenamiento sin protección
	Falta de cuidado al desecharlos
	Copia no controlada
Software	No hay pruebas de software o son insuficientes
	Fallas del software conocidas
	Sin *cierre de sesión* al salir de la estación de trabajo
	Eliminación o reutilización de los medios de almacenamiento sin el borrado adecuado
	Fata de seguimiento de la auditoría
	Asignación errónea de los derechos de acceso
	Software ampliamente distribuido
	Aplicación de programas de aplicación a los datos equivocados en términos de tiempo
	Interfaz de usuario complicada
	Falta de documentación
	Configuración incorrecta de los parámetros
	Fechas incorrectas
	Falta de mecanismos de identificación y autentificación, como la autentificación del usuario
	Tablas de contraseñas desprotegidas
	Mala gestión de las contraseñas
	Servicios innecesarios habilitados

	Software inmaduro o nuevo
	Especificaciones poco claras o incompletas para los desarrolladores
	Falta de control efectivo de los cambios
	Descarga y uso incontrolado de software
	Falta de copias de seguridad
	Falta de protección física del edificio, puertas y ventanas
	Falta de producción de informes de gestión
Red	Falta de pruebas de envío o recepción de un mensaje
	Líneas de comunicación desprotegidas
	Tráfico sensible sin protección
	Cableado de las articulaciones es deficiente
	Un solo punto de falla
	Falta de identificación y autentificación del remitente y el receptor
	Arquitectura de red insegura
	Transferencia de contraseñas en claro
	Gestión inadecuada de la red (resistencia del enrutamiento)
	Conexiones de redes públicas desprotegidas
Personal	Ausencia de personal
	Procedimiento de contratación inadecuado
	Capacitación insuficiente en materia de seguridad
	Uso incorrecto de software y hardware
	Falta de conciencia de seguridad
	Fata de mecanismos de vigilancia
	Trabajo no supervisado por personal externo o de limpieza
	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería
Sitio	Uso inadecuado o descuidado del control del acceso físico a edificios o habitaciones
	Ubicación en una susceptible de inundación
	Red eléctrica inestable
	Falta de protección física del edificio, puertas y ventanas
	Falta de procedimiento formal para el registro y la cancelación del usuario
	Falta de un proceso formal para el análisis del derecho de acceso
	Falta o insuficiencia de disposiciones (relativas a la seguridad) en los contratos con clientes y/o terceros
	Falta de procedimiento de vigilancia de las instalaciones de procesamiento de información
Organización	Falta de auditorías regulares (supervisores)
	Falta de procedimientos de identificación y evaluación de riesgos
	Falta de informe de fallos registrados en los registros del administrador y el operador
	Respuesta inadecuada del servicio de mantenimiento
	Falta o insuficiencia de acuerdo de nivel del servicio
	Falta de procedimiento de control de cambios
	Falta de procedimiento formal para el control de la documentación del SGSI
	Falta de procedimiento formal para la supervisión de los registros del SGSI

	Falta de un proceso formal para la autorización de la información disponible al público
	Falta de asignación adecuada de responsabilidades en materia de la seguridad de la información
	Falta de planes de continuidad
	Falta de política de uso del correo electrónico
	Falta de procedimientos para introducir programas informáticos en los sistemas operacionales
	Falta de registros en los registros del administrador y del operador
	Falta de procedimientos para el manejo de información clasificada
	Falta de responsabilidades en materia de seguridad de la información en las descripciones de los puestos de trabajo
	Falta o insuficiencia de disposiciones (relativas a la seguridad de la información) en los contratos de los empleados
	Falta de un proceso disciplinario definido en caso de incidente de seguridad de la información
	Falta de política formal sobre el uso de la computadora móvil
	Falta de control de los activos fuera del local
	Falta o insuficiencia de la política de *escritorio y pantalla despejados*
	Falta de autorización de las instalaciones de procesamiento de información
	Falta de mecanismo de vigilancia establecidos para las violaciones de la seguridad
	Falta de exámenes periódicos de la gestión
	Falta de procedimientos para informar de los puntos débiles de seguridad
	Falta de procedimientos de cumplimiento de las disposiciones en materia de derechos intelectuales

Tabla No. 5. Listado indicativo de vulnerabilidades relacionadas con los riesgos de la seguridad de la información. Fuente: ISO 27005:2022

El registro de los riesgos de seguridad de la información se debe realizar en la sección del mapa de riesgos y oportunidades que se muestra en la figura 5.

Código del riesgo	IDENTIFICACIÓN DE RIESGOS PARA LA SEGURIDAD DE LA INFORMACIÓN				ANÁLISIS DE RIESGO INHERENTE			
	Riesgo	Activo	Vulnerabilidad	Amenaza	Impacto		Probabilidad	Riesgo Inherente (ZIR)
					Afectación económica	Afectación reputacional	Número de veces que se realiza la actividad	
					1	1	1	Zona de Riesgo Baja

Figura No. 5 Espacio del mapa de riesgos y oportunidades destinado para el diligenciamiento de los riesgos de seguridad de la información

4.7.1 ASIGNACIÓN DEL IMPACTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Entendiendo la naturaleza de los riesgos de seguridad de la información, la asignación del nivel de impacto de este tipo de riesgos se debe realiza teniendo en cuenta los criterios establecidos por la tabla 2.

4.8 ESTIMAR EL NIVEL DEL RIESGO INHERENTE

Para estimar el nivel de riesgo inicial, los valores determinados para la probabilidad y el impacto se cruzan en la Matriz de Evaluación de Riesgo, con el fin de determinar la zona de riesgo en la cual se ubica el evento inductor identificado, registrando dicha zona en la celda respectiva del mapa de riesgos y oportunidades.

Este primer análisis del riesgo se denomina Riesgo Inherente y se define como aquél al que se enfrenta la corporación en ausencia de acciones o controles para modificar su probabilidad o impacto.

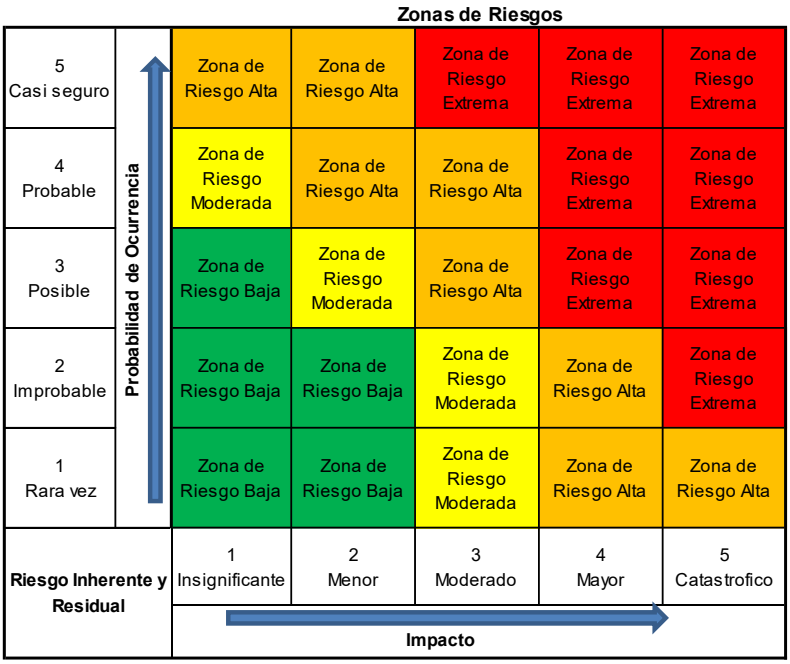


Tabla No. 6. Matriz de evaluación de riesgos

4.9 VALORACIÓN DEL RIESGO RESIDUAL

Para la valoración del riesgo residual es necesaria la identificación y registro de las acciones de control para cada uno de los riesgos identificados. Posteriormente, se valorará el nivel de eficacia que realmente tienen estas acciones sobre el riesgo. Estas acciones deben establecerse en la columna *Descripción del Control* del *Mapa de riesgos y oportunidades*.

Por lo anterior, se recomienda considerar las siguientes variables para la establecer dichas acciones de control:

- El responsable de ejecutar la actividad
- La acción controlará el riesgo
- La periodicidad de la acción.
- Fuente de información
- Evidencia generada

Posteriormente, es necesario valorar los controles establecidos, lo cual implica:

a. Determinar su **naturaleza**: Si se trata de un control de tipo preventivo, detectivo o correctivo.
b. Determinar su **modo de implementación**: Si se trata de una implementación de controles de manera automática, es decir, asistida por software o ayudas tecnológicas, o si se realiza de manera manual por parte de un colaborador.
c. Determinar si cuenta con **documentación**: Consiste en determinar si el control establecido cuenta con documentación, por ejemplo, guías, procedimientos, instructivos, manuales, o, por el contrario, no se cuenta con ningún documento que soporte la medida de control.
d. Determinar la **frecuencia** de implementación: Se debe establecer si el control se realiza de manera continua, es decir, en ciclos planificados, o si se realiza de manera aleatoria.
e. Determinar si cuenta con **evidencia** de su implementación: Se debe evaluar si la implementación del control genera las evidencias o registros suficientes para comprobar soportar su adecuada ejecución.

Acorde con lo anterior, se tienen 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 cuando se materializa el riesgo y tiene como objetivo reducir el impacto del evento.

En la tabla 7 se muestra el consolidado de los criterios de valoración de los controles establecidos por el proceso frente a los riesgos identificados. Es preciso establecer que por cada uno de los criterios solamente se puede escoger una opción, por lo tanto, el máximo puntaje que puede recibir un control es **100.**

Por ejemplo: Si un control es de tipo Preventivo (20 puntos), su implementación es automática mediante un software especializado (20 puntos), el proceso cuenta con documentación que soporta la implementación del control (20 puntos), el proceso lleva a cabo el control de manera aleatoria (10 puntos) y se dejan registros como evidencia de su implementación (20 puntos), este control recibe una valoración de **90 puntos.**

Criterios para la Evaluación de controles	Clases	Puntuación
TIPO	Preventivo	20
	Detectivo	15
	Correctivo	10
IMPLEMENTACIÓN	Automático	20
	Manual	15
DOCUMENTACIÓN	Documentado	20
	Sin documentar	10
FRECUENCIA	Continua	20
	Aleatoria	10
EVIDENCIA	Con registro	20
	Sin registro	10
PUNTAJE MÁXIMO POSIBLE		**100**

Tabla No. 7. Análisis y evaluación de controles.

Con base en la valoración del control obtenida, es necesario realizar la reducción de los cuadrantes correspondientes en el sentido de la probabilidad o el impacto, según corresponda el tipo de control, es decir, a mayor cantidad de controles preventivos y detectivos se reducirá la probabilidad, mientras que a mayor cantidad de controles correctivos se reducirá el impacto.
Para este ajuste es necesario tener en cuenta la relación que se muestra en la tabla 8.

Rangos de Calificación de los Controles	Cuadrantes a disminuir
Entre 0-65	0
Entre 66-85	1
Entre 86-100	2

Tabla No. 8. Rango de calificación de los controles.

4.10 ACCIONES EN CASO DE MATERIALIZACIÓN DEL RIESGO

A pesar de establecer e implementar controles para prevenir la materialización del riesgo, se tiene cierta posibilidad de que esto pueda suceder, por esta razón, es necesario definir acciones en caso de materialización del riesgo que busquen mitigar o contener las consecuencias negativas del evento. Estas acciones deben quedar registradas en la columna *Acciones en caso de materialización* del *Mapa de riesgos y oportunidades.*

En caso de materialización del riesgo, el personal responsable de estas acciones debe implementarlas de acuerdo con lo establecido en el *Mapa de riesgos y oportunidades* asegurando en todo momento las evidencias y registros que den soporte.

Es recomendable que posterior a un evento de materialización del riesgo, el líder del proceso (segunda línea de defensa) y el personal encargado de gestionar los riesgos identificados (primera línea de defensa) realice un análisis de la situación que le permita determinar en que fallaron los controles del riesgo y como fue la eficacia de las acciones establecidas en caso de materialización. De este análisis puede identificarse, entre otros elementos, lo siguiente:

- Deficiencias en el diseño o implementación de los controles, tanto en los controles del riesgo como en las acciones en caso de materialización.
- Necesidad de diseñar y establecer nuevos controles.
- Necesidad de documentar acciones que actualmente se implementan para controlar los riesgos.
- Necesidad de implementar cambios dentro de los procesos de la entidad.

Estas cuestiones identificadas deben gestionarse de acuerdo con los procedimientos establecidos dentro del Sistema de Gestión Integrado de la Entidad, por ejemplo:

- En caso de requerir un cambio en los procesos, se debe proceder de acuerdo con el procedimiento de Gestión del Cambio del SGI.
- Si se presentan desviaciones en la implementación de los controles se sugiere la definición de una acción correctiva de acuerdo con el procedimiento para gestionar las acciones correctivas establecido en el SGI.

Las acciones tomadas posterior al análisis de la materialización del riesgo deben ser soportadas y evidenciadas adecuadamente.

4.11 ARTICULACIÓN CON EL SISTEMA DE GESTIÓN INTEGRAL Y OTROS

Teniendo en cuenta que los procesos operan como un sistema, se debe determinar y registrar con qué indicador establecido en el proceso guarda relación el inductor de riesgo identificado y en el caso de no existir, diligenciar No Aplica (N.A.) o contemplar la posibilidad de su creación.

Por otra parte, se deben registrar los documentos establecidos en el sistema de gestión integral de la corporación que guardan relación con el inductor de riesgo identificado, en el caso de existir, en caso contrario, diligenciar no aplica (N.A.)

5. TRATAMIENTO DE RIESGOS

La C.R.A considera como apetito de riesgo a los niveles bajo y moderado. En caso de los niveles alto y extremo, estos serán objeto del plan de tratamiento como instrumento mediante el cual la entidad define las acciones que implementará para reducir, evitar, transferir o aceptar los riesgos identificados en dichos niveles.

Reducir: Implementar controles para reducir la probabilidad o el impacto.
Compartir: Compartir las consecuencias de la materialización del riesgo.
Aceptar: Cuando el nivel del riesgo está por debajo del apetito establecido por la alta dirección.
Evitar: Cuando se decide eliminar el activo que es fuente del riesgo.

Tal como se muestra en el mapa de riesgos y oportunidades, el plan de tratamiento de riesgos contemplará lo siguiente:

Descripción de la acción: En este campo se especifica la acción basada en el análisis de causas.
Responsable: En este campo se especifica el cargo de quien implementa el control.
Fecha: En este campo se especifica el inicio y la finalización de la implementación del control.

Con el objetivo de asegurar las acciones contempladas en el Plan de Tratamiento, el líder del proceso efectuará seguimientos planificados los cuales registrará en el espacio correspondiente en el formato de mapa de riesgos y oportunidades que se muestra en la figura 6.

Plan de Tratamiento								
¿Requiere plan de tratamiento?	Descripción de la Acción	Responsable (Cargo)	Fecha de Inicio	Fecha de Finalización	Seguimiento 1 (Fecha y avance)	Seguimiento 2 (Fecha y avance)	Seguimiento 3 ... (Fecha y avance)	Estado
SI								

Figura No. 6 Espacio del mapa de riesgos y oportunidades destinado para el diligenciamiento de los riesgos de seguridad de los seguimientos.

Respecto a la gestión de los riesgos de integridad, el plan de tratamiento deberá priorizar controles preventivos y detectivos orientados a evitar la ocurrencia del evento, fortalecer la transparencia y asegurar la trazabilidad de las decisiones. La aceptación del riesgo deberá sustentarse expresamente y no procederá cuando el riesgo comprometa la legalidad, la imparcialidad, la ética pública o la confianza institucional en niveles no tolerables.

6. METODOLOGÍA PARA LA GESTIÓN DE LAS OPORTUNIDADES

La operación de los procesos de la Corporación está expuesta tanto a riesgos como a oportunidades de mejora, por consiguiente, la identificación y sobre todo la evaluación de las oportunidades por parte de cada uno de los procesos cobra vital importancia en la mejora continua propuesta desde el Sistema de gestión integral de la Corporación Regional Autónoma del Atlántico.

Entendiendo la importancia de las oportunidades, se diseña el presente documento que sirve de guía para el personal de todos los procesos de la Corporación que identifiquen y necesiten evaluar la oportunidad en términos de probabilidad de consecución, relación beneficio costo, impacto sobre la seguridad y salud del trabajo, impacto sobre el desempeño ambiental e impacto sobre los servicios prestados por la Corporación.

La metodología para la identificación y evaluación de la oportunidad se fundamenta en los conceptos establecidos en las normas ISO 9001:2015, ISO 14001:2015 e ISO 45001:2018. La propuesta de las anteriores normas mencionadas se orienta

principalmente hacia el aseguramiento del logro de los resultados previstos en el Sistema de gestión integral, aumentar los efectos deseados y lograr la mejora en la organización. A continuación, se dan las directrices que debe considerar el personal de la Corporación para identificar y evaluar las oportunidades presentes en cada uno de los procesos.

6.1 IDENTIFICACIÓN DE LA OPORTUNIDAD

Para la identificación de las oportunidades, los líderes de los procesos junto con su equipo de trabajo deben considerar lo siguiente:

- El contexto interno y externo (Ver documento *Análisis del Contexto Interno y Externo de la Organización*).
- Las necesidades y expectativas de las partes interesadas (Ver documento *Análisis de partes interesadas*)

La identificación de las oportunidades del proceso se debe registrar en el *Mapa de riesgos y oportunidades* correspondiente. Para este propósito se habilitó el espacio que se muestra en la figura 6. Es preciso diligenciar la descripción general de la oportunidad, el origen o fuente de donde de identificó dicha oportunidad, así como sus posibles efectos en caso de materializarse.

IDENTIFICACIÓN DE OPORTUNIDADES DEL PROCESO		
Oportunidad	**Origen**	**Posibles Efectos**

Figura No.7. Espacio del Mapa de riesgos y oportunidades destinado para diligenciar la información de las oportunidades.

6.2 VALORACIÓN DE LAS OPORTUNIDADES

La valoración de las oportunidades se realizará en términos de **Factibilidad** y de **impacto** con el objeto de determinar el nivel de priorización que debe recibir por parte del proceso que identificó la oportunidad.

La medición de la factibilidad y del impacto cuentan con una matriz que permitirá la asignación del valor que el proceso crea adecuado.

Esta valoración quedará consignada en el espacio del Mapa de riesgos y oportunidades que se muestra en la figura 8.

VALORACIÓN DE LA OPORTUNIDAD			
Imp.	**Factibilidad**	**Nivel de oportunidad**	**Nivel de priorización**
1	1	1	Oportunidad con priorización baja

Figura No. 8. Espacio del Mapa de riesgos y oportunidades destinado para diligenciar la valoración de las oportunidades.

La valoración de la factibilidad tendrá en cuenta tres (3) niveles, los cuales se muestran detalladamente en la tabla 9.

Factibilidad		
Descriptor	**Nivel**	**Descripción**
Elevada	3	La implementación de la oportunidad es altamente factible por su pertinencia, disponibilidad de recursos y aceptabilidad

Moderada	2	La implementación de la oportunidad es factible, si bien presenta algunas dificultades por la disponibilidad de recursos y/o aceptabilidad
Baja	1	La implementación de la oportunidad es poco factible con dificultades para llevarla a cabo

Tabla No. 9. Matriz de valoración de la factibilidad de las oportunidades.

En lo relativo al impacto, también se cuenta con una escala de tres niveles para la asignación del valor. El detalle de esta escala se muestra en la tabla 10.

Impacto		
Descriptor	**Nivel**	**Descripción**
Alto	3	Impacto relevante para la estrategia de la organización y resultados previstos del sistema de gestión integral. Introduce mejoras muy significativas
Moderado	2	Impacto moderado para la estrategia de la organización y resultados previstos del sistema de gestión integral. Introduce algunas mejoras relevantes
Bajo	1	Impacto bajo para la estrategia de la organización y resultados previstos del sistema de gestión integral. No introduce mejoras importantes

Tabla No. 10. Matriz de valoración del impacto de las oportunidades.

Con la valoración de los criterios establecidos anteriormente, es posible realizar el cruce en la matriz que se muestra en la tabla 11 y de esta manera determinar si la oportunidad debe recibir prioridad baja, media o alta.

		IMPACTO		
		1	**2**	**3**
FACTIBILIDAD	**3**	Media	Media	Alto
	2	Baja	Media	Media
	1	Baja	Baja	Media

Tabla No. 11. Matriz de asignación de prioridad de las oportunidades de acuerdo con el nivel de impacto y factibilidad.

6.3 ACTIVIDADES PARA LA GESTIÓN DE LAS OPORTUNIDADES

Teniendo en cuenta la asignación del nivel de priorización realizada, el proceso debe establecer las actividades necesarias para la materialización de la oportunidad en estudio. La implementación de las actividades debe generar unos productos, los cuales se deben describir dentro del *Mapa de riesgos y oportunidades.* Finalmente, el proceso asignara un responsable para la implementación de las actividades.

Esta información se consolidará en el espacio del mapa de riesgos y oportunidades que se muestra en la figura 9.

GESTIÓN DE LAS OPORTUNIDADES		REPONSABLE
Actividades para implementación de la oportunidad	Productos entregables	

Figura No. 9. Espacio del Mapa de riesgos y oportunidades destinado para diligenciar las actividades necesarias para la gestión de las oportunidades.

7. SEGUIMIENTO, ACTUALIZACIÓN Y VERIFICACIÓN DE LOS MAPAS DE RIESGO Y OPORTUNIDADES

7.1 SEGUIMIENTO DE LOS RIESGOS Y OPORTUNIDADES

Los mecanismos de seguimiento a los riesgos y oportunidades de cada proceso deben asegurar que las acciones establecidas en los *mapas de riesgos y oportunidades* se están implementado adecuadamente.

El seguimiento de los riesgos y oportunidades, en primera instancia es responsabilidad de los líderes de los procesos, quienes son los encargados de gestionar las acciones asociadas a los controles y actividades establecidos para cada uno de los riesgos identificados en su proceso.

Durante la aplicación de las acciones de seguimiento, cada líder de proceso debe mantener la documentación respectiva de todas las actividades realizadas, para garantizar de forma razonable que los riesgos no se materialicen y las oportunidades se consoliden, y por ende que los objetivos del proceso se cumplan.

7.2 ACTUALIZACIÓN Y VERIFICACIÓN DE LOS MAPAS DE RIESGO Y OPORTUNIDADES

Los mapas de riesgos y oportunidades establecidos en cada proceso están sujetos a cambios y actualizaciones cuando se requiera, los cuales deberán ser solicitados por los líderes de proceso y consignarse en el control de cambio del *Mapa de riesgos y oportunidades* correspondiente.

Se sugiere revisar el contenido de los mapas *de riesgos y oportunidades,* cuando se presenten las siguientes situaciones:

- Materialización de un riesgo.
- Cambio normativo.
- Modificaciones sustanciales del proceso.
- Incorporación de nuevos trámites o servicios.
- Hallazgo de auditoría.
- Queja o denuncia relevante.
- Evidencia de ineficacia de un control.

La Coordinación del Sistema de Gestión Integral de la Corporación, en representación de la secretaria general, en el marco de la *Revisión por Dirección* consolidará la información relevante asociada a los mapas de riesgos y oportunidades de los procesos, con el fin de identificar acciones de mejora en la gestión del riesgos y oportunidades.

De igual forma, en el marco del *Plan Anual de Auditoría* y la implementación de las auditorías internas de gestión, la Oficina de Control Interno de la Corporación realiza revisión a los riesgos que han sido consolidados en el *Mapa de riesgo y oportunidades* de los procesos, con el fin de evaluar el diseño, efectividad e idoneidad de los controles y determinar si los riesgos se han materializado.

CONTROL DE CAMBIOS

Versión	Fecha	Descripción del Cambio
1	12/07/2019	Creación de documento.
2	13/11/2020	En la hoja de presentación se eliminó “2019”. En la Política de Administración de Riesgos se eliminó la palabra “. . . para alcanzar . . ..” En la identificación del Riesgo, se agregó “trazados en las líneas estratégicas”. En la Valoración del Riesgo, se incluye “constantemente en el año” y se elimina “al menos anualmente”. Se agrega en el subtítulo “Acciones Correctivas” la expresión “En Caso de Materialización Del Riesgo”. Se debe registrar y evidenciar la aplicación de las acciones tomadas. La aplicación de una acción efectiva puede pasar hacer parte de los controles. Si el riesgo materializado, después de haberse aplicado los controles, se encuentra en Zona de Riesgo Alto y Extremo, se debe adoptar acciones correctivas. Si se encuentra en Zona Baja y Moderada, se toman acciones de corrección y se monitorea constantemente su comportamiento, puesto que, de ser repetitivo se tendría que establecer una acción correctiva”. Se incluyó en Articulación con el Sistema de Gestión y Otros, las expresiones “colocar no aplica (N.A.)” y “en caso contrario, colocar no aplica (N.A.)”. En la parte de Elaboración del Mapa de Riesgo, se elimina “los cuales pueden afectar el logro de sus objetivos”. En la sección “Alineación con las Políticas de Lucha Contra la Corrupción y de Eficiencia Administrativa”, se eliminó el “código SJ-MP-01” y se reemplazó por “XX-MP-01”. Se eliminó la expresión “unas instrucciones” y se incluyó “descritas las pautas establecidas en la presente guía” En las secciones de Aprobación y Modificaciones, y Vigencia se reemplazó la expresión “Comité de Calidad” por “Institucional de Gestión y Desempeño”. En Mecanismos de Divulgación, se reemplazó “y/o a página web de esta (www.crautonoma.gov.co/)” por “en el proceso Gestión del Mejoramiento, código: CG-GI-01”.

		Adicionalmente, se le incluyó la nueva versión del logo del SGI.
3	28/10/2022	Se incluyeron fuentes de información para la identificación del riesgo Se elimino el establecimiento del contexto Se modifico la valoración del riesgo
4	30/08/2023	Ajuste de la política de administración de riesgos. Inclusión de terminología referente a gestión del riesgo fiscal y riesgos de seguridad de la información
5	07/05/2024	Se establece los criterios para establecer el nivel de impacto de los riesgos de corrupción. Se establece la metodología para la identificación y gestión de los riesgos de seguridad de la información. Se fusiona el documento Guía para la gestión de riesgos con el documento Guía para la gestión de oportunidades, por lo tanto, el nombre del documento cambió a Guía de gestión de riesgos y oportunidades.
6	11/03/2026	Se actualiza el documento tomando como referencia la Guía para la gestión integral del riesgo en entidades públicas en su versión 7. Se reemplaza el terminó administración por el de gestión en todo el documento. Se incluyen nuevos términos y definiciones. Se ajusta el numeral 4.1.1: Determinar la probabilidad. Se ajusta el numeral 4.1.2: Registro de riesgos institucionales. Se ajusta el numeral 4.1.2.1: Asignación del impacto de los riesgos institucionales. Se ajusta el numeral 4.1.3: Registro de riesgos de corrupción. Se ajusta el numeral 4.1.4: Registro de riesgos fiscales. Se ajusta el numeral 4.1.5: Registro de riesgos de seguridad de la información Se ajusta el numeral 4.1.5.1: Asignación del impacto de los riesgos de seguridad de la información. Se ajusta el numeral 4.1.7: Valoración del riesgo residual. Se incluye el numeral 4.4: Tratamiento de riesgos. Se ajusta el numeral 6: Seguimiento, revisión y actualización de los mapas de riesgo y oportunidades.
7	02/09/2026	Se ajusta la introducción del documento. Se ajusta la política de gestión del riesgo.

		Se incluyen nuevos términos y definiciones. Se incluye el capítulo: Gestión de riesgos para la integridad pública. Se elimina la tabla Criterios para valorar el impacto de los riesgos de corrupción. Se alinea todo el documento con la gestión de riesgos para la integridad pública. Se elimina el numeral: alineación con las políticas de lucha contra la corrupción y de eficiencia administrativa.