INFORME DE SEGUIMIENTO AL MAPA DE RIESGOS

I SEMESTRE 2026

OFICINA DE CONTROL INTERNO

JUNIO 2026

1. INTRODUCCIÓN

La Corporación Autónoma Regional del Río Grande de la Magdalena, CORMAGDALENA, desarrolla su gestión bajo el Plan de Acción 2024-2026 *"Por un río que conecte a los colombianos"*, alineado con el Plan Nacional de Desarrollo 2022-2026 y orientado a la recuperación de la navegabilidad, protección ambiental, actividad portuaria, conservación de tierras, innovación y fortalecimiento institucional; reportando avances significativos en las diferentes áreas, lo cual constituyen el principal contexto estratégico para la gestión del riesgo durante 2026.

De acuerdo con la Guía DAFP V7, la gestión del riesgo debe encontrarse articulada con la planeación institucional, gestión presupuestal, sistema de compras públicas, gobierno institucional, gestión de la información y, por supuesto, el control interno. Se observa que dentro de los diferentes componentes se resalta la planeación estratégica con un nivel avanzado de madurez, sin embargo, el marco de seguimiento de riesgo implementado presenta debilidades en la asociación de los riesgos identificados a los objetivos institucionales de la entidad, tales como los indicadores clave de riesgo

El manual metodológico instrumenta la gestión integral de riesgos y delimita las acciones de supervisión y seguimiento institucional. Bajo este marco, los líderes de proceso efectuaron la revisión exhaustiva de sus respectivas matrices, concluyendo el período sin registrar desviaciones ni hallazgos. Este ejercicio técnico validó la trazabilidad de los riesgos materializados, evaluando la efectividad de las medidas de mitigación desplegadas para salvaguardar la continuidad de las operaciones y el cumplimiento de los objetivos estratégicos de Cormagdalena.

El universo evaluado comprende 99 riesgos tipificados y distribuidos por proceso. Durante el primer semestre de 2026, el indicador de materialización se mantuvo en cero (0%), resultado que valida técnicamente la robustez e idoneidad de los controles preventivos implementados. El cierre de este documento integra el análisis analítico del comportamiento del riesgo residual y consolida recomendaciones estratégicas orientadas a blindar las barreras preventivas institucionales. Asimismo, este informe se constituye en un activo de conocimiento fundamental para la Oficina de Planeación, optimizando la articulación transversal, el entendimiento del entorno de control y la gobernanza del riesgo en Cormagdalena.

La política institucional de gestión de riesgo evidencia una alineación conceptual adecuada con MIPG; sin embargo, aún se observa una gestión predominantemente operativa y no completamente orientada al riesgo estratégico, particularmente en la gestión de la información y seguridad digital.

No obstante, la gestión basada en procesos, a partir del Manual de Administración de Riesgos bajo el código M-PAS-ADR-01 ha permitido a cada área de Cormagdalena identificar los procesos susceptibles a riesgos, evaluar la probabilidad de eventos

adversos y medir el posible impacto asociado a su ocurrencia. Gracias a estas medidas, se ha facilitado el desarrollo de estrategias preventivas para evitar la materialización de dichos riesgos y asegurar el cumplimiento de los objetivos organizacionales, como quedó registrado en informe de la anualidad precedente

2. ASPECTOS GENERALES DEL SEGUIMIENTO A RIESGOS

1.1. OBJETIVO

Realizar el seguimiento al Mapa de Riesgos institucional (procesos y corrupción) correspondiente al I semestre de 2026, con el fin de verificar la efectividad de los controles establecidos conforme al Modelo Estándar de Control Interno (MECI), la metodología DAFP y el Manual de Gestión del Riesgo de Cormagdalena.

1.2. ALCANCE

El informe abarca el análisis, evaluación y seguimiento al mapa de riesgos de la entidad, relacionando los tipos de riesgos por proceso, su materialización y el impacto de los mismos.

1.3. METODOLOGÍA

En el desarrollo del presente informe, se verificó las matrices de riesgo de procesos y de corrupción de la entidad, así como el informe de gestión de los mismos, constatando la información suministrada por el proceso de Direccionamiento Estratégico. Posteriormente, se procedió a realizar el análisis de la información obtenida, el registro de los resultados y la comunicación del informe.

2. CLASIFICACIÓN DE RIESGOS DE LOS PROCESOS DE AGENCIA

En cumplimiento de la Dimensión de Control Interno del Modelo Integrado de Planeación y Gestión (MIPG), el presente informe se fundamenta en los lineamientos metodológicos de la Guía para la Gestión Integral del Riesgo del DAFP. Bajo este estándar técnico, la arquitectura de control de la entidad se estructura mediante un portafolio de matrices que segmenta los riesgos en tres tipologías críticas: **Gestión,** asociados a la eficiencia operativa y al cumplimiento de metas de los procesos; **corrupción**, enfocados preventivamente en evitar la desviación de la función pública para fines particulares; y **seguridad de la información**, orientados a mitigar vulnerabilidades digitales que amenacen la confidencialidad, integridad y disponibilidad de los datos institucionales. La articulación sistémica de estas dimensiones permite consolidar una visión transversal del entorno de control, asegurando la mitigación oportuna del riesgo residual y blindando los objetivos de Cormagdalena.

CLASIFICACIÓN DE LOS RIESGOS MATRIZ DE LA ENTIDAD			
CONTEXTO	**RIESGO**	**EXTERNO**	**INTERNO**
Riesgo de gestión	Antijurídico	4	6
	Estratégicos	1	18
	Cumplimiento		7
	Financieros	1	5
	Operativo	6	12
	Imagen	4	1
Riesgo de corrupción	Corrupción		19
	Operativo		1
Riesgo seguridad informática	Cumplimiento		14
		16	**83**

3. RESULTADOS DEL SEGUIMIENTO A LA MATRIZ DE RIESGOS

Se realizó el seguimiento a los riesgos del I semestre de 2026 para validar el estado y las acciones implementadas sobre los mismos. Dentro del presente se resalta la materialización de un (1) riesgo de gestión consistente en la *"imposibilidad de recaudar valores adeudados"* según reporte de la Oficina Asesora Jurídica, en lo relacionado con los siguientes procesos de cobro coactivo por la ocurrencia del fenómeno de la prescripción:

Deudor	*Fecha de Prescripción*	*Valor de la Obligación con corte de marzo 202C*
José Nelson del Vasto	27/09/2019	$ 3.213.125.991,00
Drylog Astillero y Logístico	19/09/2022	$ 4.194.737.794,54
Distrito de Cartagena -	18/09/2023	$ 292.776.446,00
Juan Manuel Gálvez (QEPD):	23/05/2024	$ 292.633.356,00
Bolívar López Primavera -	24/05/2024	$ 234.782.824,30
Sociedad Portuaria Terminal de Mallorquín	25/07/2024	$ 4.003.214.587,51
Sociedad Portuaria Terminal Galán	25/07/2024	$ 89.035.842,00
Sociedad Portuaria Sociedad Portuaria de Puerto Berrio – Soportuaria	26/07/2024	$ 3.657.679.296,00
Sociedad Portuaria Parques Urbanos -	21/08/2024	$ 1.985.291.197,61
Municipio de Barranco de Loba -	6/09/2024	$ 114.343.338,00

Durante la evaluación de la Matriz de Riesgos y de los estados financieros de la Entidad, se constató la materialización del riesgo de gestión a partir de la Imposibilidad de recaudo de las obligaciones por ocurrencia del fenómeno de la prescripción. Específicamente, se identificó que una cartera ascendente a los DIECIOCHO MIL SETENTA Y SIETE MILLONES SEISCIENTOS VEINTE MIL SEISCIENTOS SETENTA Y DOS CON NOVENTA Y SEIS CENTAVOS ($18.077.620.672,96) correspondiente a los años 2019 - 2026, que no fue objeto de acciones de cobro persuasivo ni coactivo oportunas. Como consecuencia de esta inactividad administrativa, operó el fenómeno jurídico de la prescripción de la acción de cobro, extinguiendo el derecho de la Entidad pública a exigir el pago de

dichas obligaciones y convirtiendo estos saldos en cuentas incobrables que debieron ser castigadas.

Criterio

La gestión de recaudo y la administración del riesgo deben alinearse con el marco constitucional y legal vigente que castiga la negligencia administrativa. Los criterios vulnerados incluyen:

- Principio de Eficiencia y Celeridad Administrativa: Obligación de las entidades públicas de asegurar el recaudo de los caudales públicos para garantizar los fines del Estado.

- Normativa sobre Prescripción: Artículo 817 Estatuto Tributario, el cual establece un término perentorio de cinco (5) años para que la administración ejerza su facultad de cobro antes de que opere la prescripción.

- Políticas de Operación de la Matriz de Riesgos: El manual de control interno de la entidad exige la ejecución obligatoria de controles preventivos y mitigatorios (alertas tempranas, control de términos de vencimiento) para evitar que los riesgos de gestión alcancen su nivel de impacto extremo.

Causa

Un primer análisis permite inferir que la materialización de este riesgo se originó por:

- Falta de supervisión y control del área jurídica o de cobro coactivo: Inexistencia de un sistema automatizado de alertas que notifique la proximidad del vencimiento de los términos de prescripción.
- Inoperancia de los controles de la Matriz de Riesgos: Los controles definidos en la matriz se limitaron a un diseño documental formal, pero carecieron de una aplicación práctica y efectiva en el día a día operativo.
- Rotación de personal o debilidad institucional: Ausencia de un proceso riguroso de entrega de inventarios de cartera pendiente entre los funcionarios salientes y entrantes**.**

Validación de los controles de la matriz general.

Se observa controles formulados de manera genérica: “Realizar seguimiento”, “Verificar información”, “Revisar documentos”. Estos controles no demuestran reducción efectiva del riesgo. Así mismo, se evidencia debilidades en la segregación de funciones y procesos críticos como contratación, gestión

financiera y gestión documental, tratados como riesgos residuales, posiblemente subvalorados frente a controles insuficientemente documentados.

Con base en el enfoque SIGRIP incorporado por la Guía DAFP V7, la matriz requiere fortalecimiento en:

- Gestión de conflictos de interés.
- Debida diligencia de terceros.
- Riesgos de fraude.
- Riesgos de soborno.
- Riesgos asociados a integridad pública.

OBSERVACIONES OFICINA CONTROL INTERNO

La Oficina de Control Interno destaca que la revisión de la matriz de control evidencia oportunidades de mejora previamente identificadas en la auditoría técnica tales como la formulación del riesgo, identificación de causas raíz, las consecuencias, diseño de controles y la trazabilidad del riesgo residual. Se identifican riesgos redactados como consecuencias y no como eventos de corrupción, situación contraria a la metodología DAFP-SIGRIP; por otro lado, el análisis contrastó información relevante relacionados en el informe de cumplimiento del plan de acción y los riesgos relacionados:

Procesos con mayor exposición al riesgo:

La Recuperación de la navegación y dragado es el proceso más crítico de la entidad por su impacto misional y financiero.
Principales riesgos:

- Retrasos contractuales.
- Fallas en supervisión técnica.
- Incrementos de costos.
- Eventos climáticos extremos.
- Incumplimiento de cronogramas

La Gestión portuaria Presenta niveles de cumplimiento inferiores respecto a otros programas estratégicos.
Riesgos relevantes:

- Disminución de ingresos.
- Demoras regulatorias.
- Fallas en seguimiento contractual.

Gestión de proyectos y regalías Riesgos:

- Deficiencias en formulación.
- Retrasos en ejecución.
- Riesgo fiscal.

- Pérdida de recursos de cofinanciación

Riesgos de seguridad de información.

En relación a los Riesgos de Información, estos carecen de especificidad en su determinación, ya que son descrito de manera genérica como “Ausencia de documentación”, La matriz deberá integrar de manera específica los riesgos asociados a:

- Confidencialidad.
- Integridad.
- Disponibilidad.
- Trazabilidad.
- Protección de activos.

Así mismo deberá incorporar el cumplimiento de la Ley 1581 de 2012, identificando riesgos asociados a:

- Tratamiento de datos personales.
- Accesos no autorizados.
- Pérdida de información institucional.
- Exposición de información de contratistas y ciudadanos.

La trazabilidad de controles sobre datos personales podría fortalecerse mediante:

- Inventario de bases de datos.
- Clasificación de información.
- Auditorías de acceso.
- Monitoreo de incidentes.

ALERTAS Y PUNTOS CLAVE DETECTADOS

Procesos con alta concentración potencial de riesgos

Proceso	Nivel estimado
Contratación pública	Extremo
Dragado y navegabilidad	Extremo
Gestión financiera	Alto
Sistemas de información	Alto
Gestión documental	Alto
Proyectos financiados con regalías	Alto

RIESGOS EMERGENTES.

Se consideran como riesgos emergentes aquellos eventos nuevos, imprevisibles

o de reciente identificación que aún no se comprenden por completo ni se han manifestado en su totalidad. Suelen ser externos, originados por cambios tecnológicos, regulatorios, ambientales o sociales, y tienen el potencial de impactar significativamente los objetivos estratégicos de CORMAGDALENA.

Riesgo emergente de Corrupción

Elemento	Descripción
Riesgo	Manipulación de información geoespacial y técnica para favorecer decisiones contractuales o ambientales
Causa	Débil validación independiente de información técnica
Consecuencia	Favorecimiento indebido, investigaciones disciplinarias y detrimento patrimonial

Justificación:
La entidad depende cada vez más de información geográfica, modelaciones hidráulicas y sistemas SIG para la toma de decisiones.

Riesgo emergente de Gestión

Elemento	Descripción
Riesgo	Incumplimiento de metas institucionales por eventos climáticos extremos asociados al cambio climático
Causa	Variabilidad hidrológica creciente
Consecuencia	Retrasos en dragado, obras y ejecución presupuestal

Justificación:
La misión institucional depende directamente de condiciones hidrológicas y ambientales del Río Magdalena.

Riesgo emergente de Seguridad de la Información

Elemento	Descripción
Riesgo	Ataque ransomware sobre plataformas institucionales críticas
Causa	Incremento de amenazas cibernéticas y vulnerabilidades tecnológicas
Consecuencia	Interrupción operacional, pérdida de información y afectación reputacional

Justificación:
La modernización tecnológica y los nuevos sistemas institucionales aumentan la superficie de exposición digital.

4. CONCLUSIONES

El seguimiento realizado al mapa de riesgos de Cormagdalena durante el primer semestre de 2026 evidencia la materialización de un (1) riesgo de gestión consistente en la “imposibilidad de recaudar valores adeudados” generando un

Impacto Financiero ante la pérdida definitiva de recursos líquidos para el presupuesto de la Entidad, lo que reduce la capacidad de inversión en programas sociales o de infraestructura, entre otros; así mismo, un impacto Contable y la consecuente necesidad de depurar la cartera mediante el castigo de cuentas, distorsionando la realidad financiera y reflejando una gestión ineficiente de los activos de CORMAGDALENA.

Por otro lado, se evidencian vacíos entre las estrategias institucional y los riesgos identificados en la matriz general, lo cual denota brechas entre las prioridades estratégicas de la entidad y la cobertura de riesgos entorno a la trasformación digital, gobierno de datos, ciberseguridad avanzada, analítica y sistemas SIG.

- CORMAGDALENA presenta una estructura de administración del riesgo funcional y alineada parcialmente con la Guía DAFP V7.
- La mayor exposición institucional se concentra en contratación, dragado, proyectos estratégicos, gestión financiera y sistemas de información.
- Los riesgos de corrupción muestran una madurez intermedia, requiriendo fortalecimiento en controles, segregación de funciones y gestión de integridad.
- Los riesgos de gestión presentan debilidades metodológicas en formulación, valoración residual e indicadores de efectividad.
- Los riesgos de seguridad de la información requieren evolucionar hacia un modelo basado en activos, amenazas y vulnerabilidades conforme al MSPI[1] y la Guía DAFP V7.
- Se identifican riesgos emergentes asociados a ciberseguridad, cambio climático y manipulación de información técnica que deberían incorporarse formalmente en la matriz institucional 2026.
- La Oficina de Control Interno debe priorizar un monitoreo continuo basado en KRI, auditoría basada en riesgos y validación periódica de la efectividad de los controles para fortalecer la gobernanza institucional del riesgo durante el segundo semestre de 2026.

5. RECOMENDACIONES

Acciones preventivas prioritarias

Riesgos de Corrupción

Acción	Prioridad
Implementar matriz de conflictos de interés	Alta
Segregación obligatoria de funciones críticas	Alta
Auditorías aleatorias de contratación	Alta
Debida diligencia ampliada a contratistas	Alta

[1] El **MSPI** son las siglas del Modelo de Seguridad y Privacidad de la Información. Es un marco de lineamientos del Gobierno de Colombia, diseñado por el Ministerio de las TIC (MinTIC), para ayudar a las entidades públicas a proteger sus activos digitales y gestionar riesgos.

Riesgos de Gestión	
Acción	**Prioridad**
Fortalecer supervisión y controles procesos de cobro coactivo.	Alta
Reestructurar riesgos bajo metodología DAFP V7	Alta
Incorporar Indicadores Clave de Riesgo (KRI)[2]	Alta
Revisar coherencia inherente-residual	Alta
Formalizar evaluación de eficacia de controles	Alta

Riesgos de Seguridad de la Información	
Acción	**Prioridad**
Inventario integral de activos de información	Alta
Implementación de RBAC[3] y mínimo privilegio	Alta
SIEM[4] y monitoreo continuo	Alta
Pruebas periódicas de recuperación de backups	Alta
Programa de concientización en ciberseguridad	Alta

Cordialmente,

ALBERT LUIS ALFARO CONEO
JEFE DE CONTROL INTERNO

Proyecto: **Jean C. López**
Abogado Contratista
Oficina de Control Interno

Gabino José Mora Vargas

Abogado Contratista
Oficina de Control Interno

[2] **KRI** (Key Risk Indicator) o Indicador Clave de Riesgo es una métrica que permite medir, monitorear y anticipar el comportamiento de un riesgo antes de que este se materialice. Según la Guía para la Gestión Integral del Riesgo DAFP Versión 7 (2025), los KRI son herramientas fundamentales para la toma de decisiones porque suministran información sobre riesgos emergentes, tendencias y señales de alerta temprana que pueden afectar el cumplimiento de los objetivos institucionales.

[3] Control de Acceso Basado en Roles (**RBAC** por sus siglas en inglés) es un modelo de seguridad informática que restringe el acceso a sistemas, aplicaciones y datos, asignando permisos basados exclusivamente en el rol o puesto de trabajo que ocupa cada usuario dentro de la organización.

[4] El **SIEM** (por sus siglas en inglés, *Security Information and Event Management* o Gestión de Información y Eventos de Seguridad) es una solución de ciberseguridad que centraliza y analiza registros de datos de toda la red para identificar amenazas