PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 1.0

CORPORACIÓN AUTÓNOMA REGIONAL DEL RIO GRAN DE LA MAGDALENA
CORMAGDALENA

2025

Contenido

1. INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad y privacidad de la Información de CORMAGDALENA establece una estrategia, acciones y medidas preventivas para reducir los riesgos y mantenerlos en un nivel residual aceptable para la Corporación. Esto se logra mediante la identificación, análisis, tratamiento, evaluación y monitoreo periódico de los riesgos de seguridad de la información en todos los procesos de la entidad.

Este plan tiene como objetivo desarrollar y fortalecer en CORMAGDALENA una cultura organizacional orientada al entendimiento de los riesgos y su contexto, promoviendo la prevención en todos los niveles. Se enfoca en comprender las nuevas formas de ciberataques dirigidos a entidades públicas, privadas, proveedores de servicios de TI y otros actores del ecosistema de la información pública, que se han convertido en un blanco para los ciberdelincuentes. Estos ataques pueden generar interrupciones operativas, pérdidas, robos, destrucción y daños en los servicios dirigidos a los ciudadanos. En los últimos años, estos incidentes han sido ampliamente divulgados, con el fin de fortalecer las capacidades de respuesta y el conocimiento de los mecanismos de protección ante ciberataques, fomentando una cultura de autoprotección y el manejo adecuado de la información y los datos personales.

En base a lo anterior, se presenta el Plan de Tratamiento de Riesgos de Seguridad 2025, con sus respectivas actividades, conforme a lo establecido en el Decreto 612 de 2018.

2. OBJETIVO

Definir y desarrollar una estrategia integral y actividades específicas dentro del Plan de Tratamiento de Riesgos de Seguridad de la Información de CORMAGDALENA, alineadas a la metodología de Gestión del Riesgo de la Entidad y en conformidad con los lineamientos establecidos por el Departamento Administrativo de la Función Pública (DAFP) y el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), con el fin de gestionar y mitigar los riesgos de seguridad de la información, garantizando la protección de la confidencialidad, integridad y disponibilidad de la información en todos los procesos de la entidad.

3. OBJETIVOS ESPECÍFICOS

- Identificar y actualizar los riesgos de seguridad de la información de CORMAGDALENA, mediante un proceso continuo de monitoreo y evaluación, para garantizar que todos los riesgos sean reconocidos y gestionados de manera adecuada.

- Gestionar los riesgos de seguridad de la información conforme al análisis, evaluación y valoración de estos, para asegurar la preservación de la integridad, disponibilidad y confidencialidad de los activos de información de CORMAGDALENA

- Proponer controles que apunten a minimizar la probabilidad de materialización de los riesgos identificados, estableciendo medidas preventivas y correctivas eficaces para mitigar los impactos potenciales.

- Sensibilizar y reforzar la protección y adecuado tratamiento de los activos de información y sus riesgos de seguridad, mediante charlas y socializaciones que fomenten una cultura organizacional enfocada en la seguridad de la información.

4. ALCANCE

El plan de tratamiento de riesgos de seguridad se aplica a toda la Entidad y tiene como objetivo gestionar y abordar todos los riesgos de seguridad de la información, especialmente aquellos clasificados en las categorías de riesgo extremo, alto o moderado, que exceden el nivel de apetito de riesgo aceptable en CORMAGDALENA. Su propósito es establecer mecanismos de prevención y mitigación, así como fortalecer la toma de decisiones y prevenir la materialización de incidentes de seguridad que puedan afectar el cumplimiento de los objetivos institucionales.

Para asegurar un manejo adecuado de los riesgos, es fundamental la participación de todas las áreas de CORMAGDALENA, con el objetivo de comprender, adoptar e implementar las directrices y políticas establecidas, además de realizar el seguimiento y monitoreo conforme a la Política de Riesgos de la Entidad.

5. DEFINICIONES

- **Alta dirección:** persona o grupo de personas que dirige y controla una organización, al nivel más alto (ISO/IEC 27001:2013).
- **Activo de Información:** un activo de información es, cualquier elemento que contenga, genere, adquiera, gestione y/o procese información, que tiene valor para uno o más procesos de la organización y debe protegerse (ISO/IEC 27001:2013).
- **Aceptación de riesgo:** decisión de asumir un riesgo Amenazas: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Amenaza**: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).
- **Análisis de Riesgo:** uso sistemático de la información para identificar fuentes y estimar el riesgo (Guía ISO/IEC 73:2002).
- **Apetito al riesgo:** magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.
- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Control o medida:** acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.
- **Evaluación del riesgo:** proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.
- **Gestión de riesgos:** actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y su tratamiento. (ISO 27000, Glosario de términos y definiciones).
- Impacto: son las consecuencias que genera un riesgo una vez se materialice.
- **Mapa de riesgos:** documento con la información resultante de la gestión del riesgo.
- **Probabilidad:** es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- **Riesgo:** es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.
- **Riesgo de seguridad de la información:** combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad

territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

- **Riesgo inherente:** nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.
- **Riesgo residual:** nivel restante de riesgo después del tratamiento del riesgo.
- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

6. MARCO NORMATIVO

Directiva Presidencial 02: Febrero 24 de 2022, “Para garantizar la implementación segura de la Política de Gobierno Digital liderada por el Ministerio de Tecnologías de la Información y las comunicaciones (MinTIC)”.
Decreto 338: Marzo 8 de 2022, "Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones".
Resolución 746: Marzo 11 de 2022, "Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021".
Decreto 767: Mayo 16 de 2022, “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.
Directiva Presidencial 03: Marzo 15 de 2021, “Lineamientos para el uso de Servicios en la Nube, Inteligencia Artificial, Seguridad digital y Gestión de Datos”.
Resolución 500: Marzo 10 de 2021, "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital".
Conpes 3995: Julio 1 de 2020, Política Nacional de Confianza y Seguridad Digital “Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y laactualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías”.
Resolución 1519: Agosto 24 de 2020, “Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos”.

Guía para la administración del riesgo y el diseño de controles en entidades públicas -V6: Noviembre 2022, **“**Establece la metodología para la administración del riesgo, los criterios para el análisis de probabilidad e impacto identificado y su respectivo nivel de severidad. En la versión 5 se actualizaron y precisaron algunos elementos metodológicos para mejorar el ejercicio de identificación y valoración del riesgo”.

Decreto 612: Abril 4 de 2018, “Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado”.

Decreto 1008: Junio 14 de 2018, “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto número 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.

Ley 1915: Julio 12 de 2018, “Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos”.

Decreto 103 de 2015: Enero 20 de 2015, “Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones”.

Decreto 1068: Mayo 26 de 2015, “Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Capítulo 26.

Ley 1712: marzo 06 de 2014, “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”.

Decreto 886: mayo 13 de 2014, “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos”.

Decreto 1377: junio 23 de 2013, “Por el cual se reglamenta parcialmente la Ley 1581 de 2012”.

Ley 1581: octubre 17 de 2012, “Por la cual se dictan disposiciones generales para la protección de datos personales. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013”.

Ley 1273: enero 05 de 2009, “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

7. GUÍA DE ADMINISTRACIÓN DEL RIESGO

Cormagdalena, consciente de la responsabilidad e importancia de gestionar los riesgos asociados a los procesos definidos en el Sistema Integrado de Gestión, ha implementado la Guía de Administración del Riesgo. Esta herramienta

estratégica y de gestión permite valorar y tratar los riesgos identificados en el mapa, anticipándose a su posible materialización y respondiendo de manera oportuna y eficaz. De este modo, se contribuye al cumplimiento de los objetivos misionales y se promueve la mejora continua de la entidad.

8. OBJETIVOS DE LA POLITICA DE ADMINISTRACIÓN Y GESTIÓN DE RIESGOS.

Gestionar integralmente los riesgos del Sistema Integrado de Gestión mediante el uso del Mapa de Riesgos, garantizando su control, evaluación, tratamiento y monitoreo continuo.

- Proveer a Cormagdalena las directrices necesarias para la administración efectiva de los riesgos asociados a los procesos de la entidad, con el objetivo de facilitar su adecuada identificación, análisis, valoración (incluyendo riesgos y controles) y tratamiento.
- Integrar la gestión de riesgos relacionados con la administración, corrupción, medio ambiente y seguridad de la información.
- Definir las responsabilidades de los líderes de los procesos dentro de CORMAGDALENA.
- Determinar los roles específicos de las diferentes dependencias del CORMAGDALENA.
- Asegurar el cumplimiento de los requerimientos legales aplicables al manejo de riesgos de gestión, corrupción, ambientales y de seguridad de la información.
- Promover el fortalecimiento del comportamiento ético y profesional de los funcionarios de CORMAGDALENA.

9. ESTRATEGIA DE DESARROLLO DEL PLAN

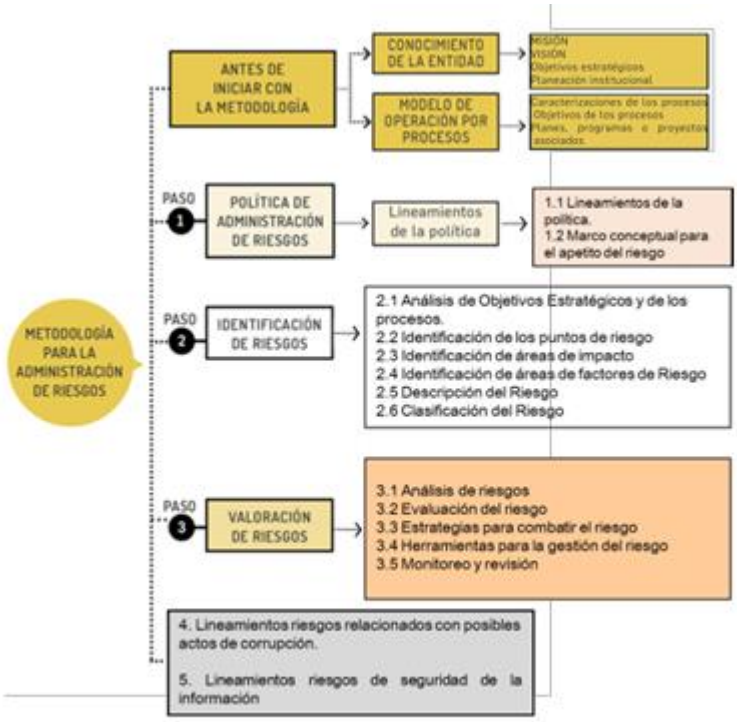
El Plan de Tratamiento de Riesgos de Seguridad de la Información establece actividades dirigidas a gestionar los riesgos de este ámbito con el objetivo de prevenir su materialización y asegurar que su valoración sea aceptable. Busca reducir las calificaciones de riesgo clasificadas como Extrema o Alta, manteniéndolas en niveles Moderados o Bajos siempre que sea posible.

La etapa de implementación se enfoca en la ejecución y cumplimiento de las actividades y objetivos definidos, considerando los roles, responsabilidades y plazos establecidos en la Política de Administración del Riesgo de la entidad. El objetivo principal de esta fase es lograr una adecuada implementación y cumplimiento de las acciones programadas.

Este plan se fundamenta en las directrices establecidas en:

La Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (V6), emitida por el Departamento Administrativo de la Función Pública (DAFP).
La Guía de Administración de Riesgos de Cormagdalena.

A continuación, se presenta el modelo de gestión de riesgos de seguridad de la información, diseñado para su adecuada administración y gestión. Los elementos que lo conforman son:



Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

10. DESARROLLO METODOLÓGICO

Teniendo en cuenta el ciclo PHVA (Planificar, Hacer, Verificar y Actuar) como base para garantizar un ciclo de mejora continua en la gestión y tratamiento de riesgos, se establecen las siguientes fases y actividades:

- Planificar: Dentro de esta etapa se llevan a cabo las actividades definidas en la fase 1 de la metodología de tratamiento de riesgos, enfocadas en la Planificación.

- Hacer: En este paso del ciclo de vida, se ejecutan las actividades correspondientes a la fase 2 de la metodología de tratamiento de riesgos, enfocada en la Implementación (Hacer).

- Verificar: En esta etapa, correspondiente a la fase 3 de la metodología de tratamiento de riesgos, se desarrollan las actividades destinadas a realizar el seguimiento y auditorías a la ejecución de las medidas implementadas.

- Actuar: Se llevan a cabo las mejoras basadas en los resultados del seguimiento, auditorías y revisiones realizadas a los riesgos de seguridad de la información.

Fase 1: Análisis de la información.
En esta fase, se analizan los resultados obtenidos en las mesas de trabajo realizadas con los diferentes procesos de la Entidad, permitiendo desarrollar las siguientes actividades:

- Verificar y analizar los riesgos identificados.
- Determinar los controles aplicables a cada riesgo.
- Definir los planes de tratamiento de los riesgos que superen al apetito aceptable.

Fase 2: Desarrollo de las medidas de tratamiento de riesgos.
En esta fase se realizarán las siguientes actividades:

- Determinar la medida de tratamiento.
- Definir los responsables de cada medida.
- Establecer el objetivo de cada medida.
- Desarrollar las actividades de ejecución de cada medida.

Fase 3: Análisis de los riegos y medidas aplicadas.
En esta fase se realizarán las siguientes actividades:

- Validar la eficacia de los controles y medidas de mitigación y tratamiento.
- Analizar la aplicabilidad de las medidas de mitigación y tratamiento.

Fase 4: Ciclo de vida del tratamiento de riesgos.
En esta fase se realizarán las siguientes actividades:

- Definir las actividades dentro del ciclo de vida del Plan De Tratamiento de riesgos.

11. Cronograma de Actividades del Plan De Tratamiento de Riesgos de seguridad y privacidad de la información.

N°	Actividad	Evidencia	Fecha Inicio	Fecha Fin	Responsable
1	**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD PRIVACIDAD DE LA INFORMACIÓN**				
1.1	Definir el Plan de Tratamiento de Riesgos de Seguridad de la Información	Plan de Tratamiento publicado /URL de publicación	ENERO 2025	ENERO 2025	EQUIPO TIC
1.2	Publicar el Plan de Tratamiento de Riesgos de Seguridad de la Información	Plan de Tratamiento publicado /URL de publicación	ENERO 2025	FEBRERO 2025	Equipo TIC/ Comunicaciones
2.	**RIESGOS DE LA SEGURIDAD DE LA INFORMACION**				
2.1	Apoyar cuando se requiera la actualización de la metodología, guía, instrumento o lineamientos de Riesgos de Seguridad de la Información.	Correo electrónico de aprobación o url de publicación del documento.	Cuando este se requiera	Cuando este se requiera	Equipo TIC
2.2	Apoyar cuando se requiera la actualización de los Riesgos de Seguridad de la Información	Mapa de riesgos	Cuando este se requiera	Cuando este se requiera	Equipo TIC/ OAP
2.3	Consolidar mapa de Riesgos de Seguridad de la Información	Mapa de riesgos consolidado	Cuando este se requiera	Cuando este se requiera	Equipo TIC
2.4	Aceptación y aprobación de los Riesgos de Seguridad de la Información y sus planes de tratamiento por parte de los procesos y/o el comité	Acta o correo de aprobación de riesgos	Cuando este se requiera	Cuando este se requiera	Lideres de cada proceso de la entidad.

12. GESTIÓN DE RIESGOS DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Es un proceso continuo cuyo objetivo es identificar los riesgos, vulnerabilidades, causas, amenazas, impactos, consecuencias, controles y las acciones de tratamiento correspondientes para cada riesgo que ha sido analizado y evaluado.

12.1. IDENTIFICACIÓN DEL RIESGO

Para gestionar los riesgos, es fundamental identificarlos, lo que implica determinar y analizar los eventos que podrían ocurrir y sus posibles repercusiones. Es necesario tener en cuenta factores como la infraestructura, las áreas de trabajo, el entorno y el ambiente. Además, cada proceso debe contar con una identificación clara de sus activos de información para una gestión efectiva.

12.2. VALORACIÓN DEL RIESGO

Se definen los criterios para evaluar la probabilidad y el impacto del riesgo identificado, así como su nivel de severidad, con un enfoque centrado en la exposición al riesgo. Este análisis proporciona a los líderes de los procesos elementos objetivos para tomar decisiones informadas. Se consideran principalmente los efectos económicos y reputacionales en caso de que los riesgos se materialicen, utilizando una escala de severidad dividida en cinco niveles (baja, moderada, alta, extrema). Además, este análisis promueve una evaluación más profunda de los riesgos, teniendo en cuenta el entorno dinámico y cambiante de la Entidad.

En las mesas de trabajo con los procesos, se lleva a cabo la identificación de los riesgos y se realiza un análisis preliminar de la probabilidad e impacto para valorar el nivel del riesgo inherente. Durante este proceso, se asocian las vulnerabilidades correspondientes y se identifican los controles necesarios para mitigarla.

12.3. TRATAMIENTO ZONA DE RIESGO FINAL

- **Zona de riesgo baja:** Aceptar el riesgo.
- **Zona de riesgo Moderada:** Aceptar el riesgo, reducir el riesgo.
- **Zona de riesgo alta:** Reducir el riesgo, evitar, transferir o compartir.
- **Zona de riesgo extrema:** Reducir el riesgo, evitar, transferir o compartir.

Los riesgos clasificados en la zona baja se consideran aceptables (según el apetito del riesgo) y se procede con su monitoreo continuo para asegurar que las condiciones bajo las cuales fueron evaluados no hayan cambiado. En caso de que las condiciones varíen, será necesario reevaluar el riesgo y, si corresponde, definir el manejo adecuado mediante los controles necesarios. Por otro lado, los riesgos relacionados con la corrupción no pueden ser aceptados en ninguna circunstancia, y deben ser tratados de manera inmediata y apropiada.

Los riesgos ubicados en las zonas más altas o de mayor gravedad son los que se priorizan, reduciendo su nivel de aceptación. Para estos riesgos, se establecen en el plan de contingencia las actividades de control correctivas, enfocadas en abordar las causas del riesgo en el caso de que se materialice.

Esto permite a la Entidad optimizar su gestión de riesgos, concentrando los esfuerzos y las acciones en aquellos riesgos que podrían tener un impacto mayor.

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

12.4. APROBACIÓN DE MAPAS DE RIESGO.

Una vez finalizadas las etapas de identificación, actualización y gestión de los riesgos de seguridad de la información, y después de completar los campos requeridos y el plan de tratamiento cuando corresponda, los líderes de los procesos deberán emitir o responder con la aprobación correspondiente. Esto incluirá un correo electrónico que adjunte el acta de aprobación de los riesgos y la matriz de riesgos asociada**.**

13. MATERIALIZACIÓN DEL RIESGO.

Cuando se detecte la materialización de los riesgos, se realizarán las siguientes acciones:

1) Materialización de riesgos detectada por parte del líder del proceso (primera línea de defensa):

• Si el riesgo es de corrupción se deberá informar a la Oficina Asesora de Planeación. Sobre el hecho encontrado. De considerarlo necesario, realizar la denuncia ante el ente de control respectivo.

• Si el riesgo es de gestión, se deberá realizar el análisis de causas y determinar acciones, análisis y actualización del mapa de riesgos.

2) Materialización de riesgos detectada por la Oficina Asesora de Planeación (segunda línea de defensa):

En los casos de riesgos de corrupción detectado por la segunda Línea de defensa, se debe:

- Informar sobre el hecho encontrado a la Oficina de Control Interno, para lo de su competencia.
- Informar al líder del proceso, para revisar el mapa de riesgos y sus controles asociados, verificar que se tomaron las acciones y que se actualizó el mapa de riesgo. •

En los casos de riesgos de Gestión detectado por la segunda Línea de defensa, se debe comunicar a la Oficina de Control Interno, para lo de su competencia y al líder del proceso sobre el hecho encontrado, para que realice la revisión, análisis y acciones correspondientes para resolver el hecho y verificar que se tomaron las acciones, que se actualizó el mapa de riesgos correspondiente e informar a la Alta Dirección sobre el hallazgo y las acciones tomadas.

3) Materialización de riesgos detectada por parte de la Oficina de Control Interno (tercera línea de defensa).

- Si el riesgo es de corrupción, se deberá convocar al Comité de Coordinación de Control Interno e informar sobre los hechos detectados, desde donde se tomarán las decisiones para iniciar la investigación de los hechos. Dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante el ente de control respectivo. Facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos y sus controles asociados. Verificar si se tomaron las acciones y si se actualizó el mapa de riesgos.

- Si el riesgo es de gestión, informar al líder del proceso sobre el hecho encontrado y orientarlo frente a la revisión, análisis y acciones correspondientes para resolver el hecho. Convocar al Comité de

Coordinación de Control Interno e informar sobre la actualización realizada.

14. OPORTUNIDAD DE MEJORA

Es necesario identificar las brechas y oportunidades de mejora en la gestión de los riesgos, teniendo en cuenta las observaciones y recomendaciones de la Oficina de Control Interno y/o los resultados de las auditorías. Este análisis permitirá optimizar el proceso de gestión de riesgos, asegurando que las estrategias y medidas adoptadas sean más efectivas y alineadas con las mejores prácticas y estándares de control interno**.**

15. RECURSOS.

Cormagdalena contará con los siguientes recursos para gestionar los riesgos de seguridad de la información**:**

RECURSOS	DESCRIPCION
Humanos	• La Secretaría General, mediante el área de sistemas y su equipo de Seguridad de la Información, tiene la responsabilidad de liderar, definir e implementar políticas y directrices en materia de seguridad de la información. Esto incluye establecer estrategias y procedimientos que apoyen la mejora continua de la seguridad y privacidad de los datos. • Los responsables de los procesos y dependencias deben asignar el personal adecuado y suficiente para llevar a cabo la identificación y gestión de los riesgos relacionados con la seguridad de la información.
Técnicos	• Política de administración y gestión de riesgos de Cormagdalena. • Herramientas para la gestión del riesgo.
Logísticos	• Recursos y logística para la transferencia de conocimiento, socializaciones y seguimiento a la gestión de riesgos.
Financieros	• Recursos asignados a Seguridad de la Información en la vigencia presupuestal del 2025.

CONTROL DE CAMBIOS

Fecha	Versión	Descripción Del Cambio
31-01-2025	Versión 1	Elaboración del Plan