REPÚBLICA DE COLOMBIA

COPNIA

Consejo Profesional Nacional de Ingeniería

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

2024 - 2026

www.copnia.gov.co

TABLA DE CONTENIDO

1. INTRODUCCIÓN 3
2. MARCO NORMATIVO 3
3. MISIÓN Y VISIÓN DE LA ENTIDAD 3
4. DEFINICIONES 4
5. OBJETIVOS 5
6. ALCANCE 5
7. MARCO REFERENCIAL 6
7.1. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS 6
8. METODOLOGÍA 7
9. RECURSOS 12
10. PRESUPUESTO PARA LA IMPLEMENTACIÓN DE CONTROLES 13
11. MEDICIÓN 13
12. ANEXOS 14
13. CONTROL DE CAMBIOS 14

1. INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y Seguridad Digital del COPNIA, contenido en **el mapa de riesgos de seguridad digital,** se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización; adicionalmente, busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el Entorno TIC para el Desarrollo Digital, ciudadanos y demás actores empoderados del Entorno Digital y de la Transformación Digital.

Lo anterior, dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3995 de 2020, Modelo de Seguridad y Privacidad del Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, a la Resolución 500 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 adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas – Riesgos de gestión, corrupción y seguridad digital, establecidos en el Modelo Integrado de Planeación y Gestión.

2. MARCO NORMATIVO

El marco normativo se toma como referencia en lo aplicable a la naturaleza jurídica del COPNIA, consignado en el portal web institucional en el siguiente link:

- Marco Normativo:

https://www.copnia.gov.co/nuestra-entidad/normatividad

3. MISIÓN Y VISIÓN DE LA ENTIDAD

Se toma como referencia en lo aplicable a la misión y visión consignados en el portal web institucional en los siguientes enlaces:

https://www.copnia.gov.co/nuestra-entidad/quienes-somos

MISIÓN:

Somos la autoridad pública encargada de velar por el buen ejercicio profesional de los ingenieros, profesionales afines y auxiliares, mediante la autorización, inspección, vigilancia y control, que

se concreta con la administración del Registro Profesional, del Registro Único Nacional de Profesionales Acreditados y con la función de Tribunal de Ética Profesional. Resolución R2022039275 del 21 de octubre de 2022

VISIÓN:

En el año 2026, seremos una entidad reconocida por la prestación del servicio con calidad y oportunidad, por el fortalecimiento de la relación con los profesionales inscritos en los Registros y con los demás grupos de interés, promoviendo la cultura ética en el ejercicio profesional, apoyados en el uso de tecnologías de la información, la gestión efectiva de las comunicaciones y el compromiso y responsabilidad de todos los funcionarios con el servicio a la ciudadanía. Resolución R2022039275 del 21 de octubre de 2022

Objetivos estratégicos de la entidad:

1. Mejorar la cobertura, oportunidad y calidad en la prestación de los servicios misionales.
2. Consolidar el Modelo de Gestión de la entidad para mejorar la prestación de los servicios misionales.
3. Fortalecer y articular las relaciones interinstitucionales y la comunicación con los diferentes grupos de interés de la Entidad.

https://www.copnia.gov.co/transparencia/plan-estrategico

4. DEFINICIONES

Los lineamientos conceptuales que enmarcan el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información son los siguientes:

- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
- **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).
- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.
- **Probabilidad:** se entiende como la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.
- **Impacto:** consecuencias que puede ocasionar a la organización la materialización del riesgo.

- **Medida:** En el contexto de la seguridad de la información es la determinación dentro de un proyecto o un proceso de las acciones a realizar y sus responsables en cuanto a salvaguardar la seguridad y privacidad de la información.

- **Control:** Mecanismos implementados para reducir o mitigar un riesgo.

- **SGSI:** Sistema de gestión de seguridad de la información.

- **MPSI:** Modelo de privacidad y seguridad de la información-

- **Riesgos de Seguridad y Privacidad de la Información:** Para la entidad COPNIA están consolidados en la matriz de riesgos del proceso de seguridad y privacidad de la información en el SGC (Sistema de Gestión de Calidad) el cual cuenta con metodología alineada a ISO 9001.

- **Riesgos de seguridad digital:** para la entidad COPNIA están consolidados en el mapa de riesgos de seguridad digital, que hacen parte del SGSI (Sistema de Gestión de seguridad de la información) de la entidad alineado a la ISO 27001:2013, cuya metodología está descrita en el presente documento.

5. OBJETIVOS

- Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, contenidos en **el mapa de riesgos de seguridad digital,** a los que el COPNIA pueda estar expuesto, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad, privacidad y autenticidad de la información.

- Cumplir con los requisitos legales, reglamentarios, regulatorios y de las normas técnicas colombianas.

- Gestionar los riesgos de riesgos de Seguridad y Privacidad de la información y riesgos de Seguridad Digital, de acuerdo con los contextos establecidos en la Entidad.

- Fortalecer y apropiar conocimiento referente a la gestión de riesgos de Seguridad y Privacidad de la información y seguridad digital, del COPNIA.

6. ALCANCE

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información y riesgos de Seguridad Digital, contenidos en **el mapa de riesgos de seguridad digital,** que permita integrar en los procesos de la entidad buenas prácticas que contribuyan a la toma de decisiones

y prevenir incidentes que puedan afectar el logro de los objetivos. Adicionalmente, dar los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información y riesgos de Seguridad Digital en el COPNIA.

El Plan de Tratamiento de Riesgo tendrá en cuenta todos los riesgos, en especial los que se encuentren en los niveles Moderado, Alto y Extremo, acorde con los lineamientos definidos por el COPNIA.

7. MARCO REFERENCIAL

7.1. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La Entidad, a través de la Resolución 1252 de 2018 adoptó la Política de Administración del Riesgo del Consejo Profesional Nacional de Ingeniería – COPNIA, con la cual, la Entidad se compromete a mantener una cultura de la administración de gestión del riesgo, orientada a la prevención y mitigación de aquellos sucesos que puedan afectar el cumplimiento de sus objetivos, a través de la implementación de instrumentos y mecanismos para su manejo y tratamiento.

Por lo anterior, a través del Sistema de Gestión de Seguridad de la Información (SGSI) se adoptan, ejecutan y promueven políticas, planes, programas, iniciativas y proyectos del sector TIC, mediante mecanismos, sistemas y controles que detecten hechos asociados, de manera Integral, con la estrategia, la gestión la transparencia y ética, la seguridad y privacidad de la información, seguridad digital y continuidad de la operación, que puedan afectar el cumplimento de los objetivos institucionales, el aprovechamiento al máximo los recursos destinados y la atención a nuestros grupos de interés.

El objetivo de la política es establecer los lineamientos generales de actuación para el control y la gestión de los riesgos, conforme a la naturaleza jurídica de la Entidad, su marco estratégico y el alcance definido en la política de administración de riesgos. Por ende, por medio del presente plan se definen los parámetros necesarios para una adecuada gestión de los riesgos de Seguridad y Privacidad de la Información y Seguridad Digital del COPNIA, contenidos en **el mapa de riesgos de seguridad digital,** procurando que no se materialicen, atendiendo los lineamientos establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP, y el procedimiento interno DE-pr-02 Administración del riesgo, orientando a la toma de decisiones oportunas y minimizando efectos adversos al interior de la Entidad, con el fin de dar continuidad a la gestión institucional y asegurar el cumplimiento de los compromisos con los Grupos de interés.

El tratamiento de riesgos es la respuesta establecida por la primera línea de defensa, es decir, los subdirectores, jefes de dependencias y líderes o responsable del proceso junto con su equipo de trabajo para la mitigación de los diferentes riesgos.

El tratamiento o respuesta dada al riesgo se enmarca en las siguientes categorías:

Aceptar el riesgo: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción es aceptado). La aceptación del riesgo puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y, por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

Reducir el riesgo: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. Deben seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

Evitar el riesgo: Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

Compartir el riesgo: Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización.

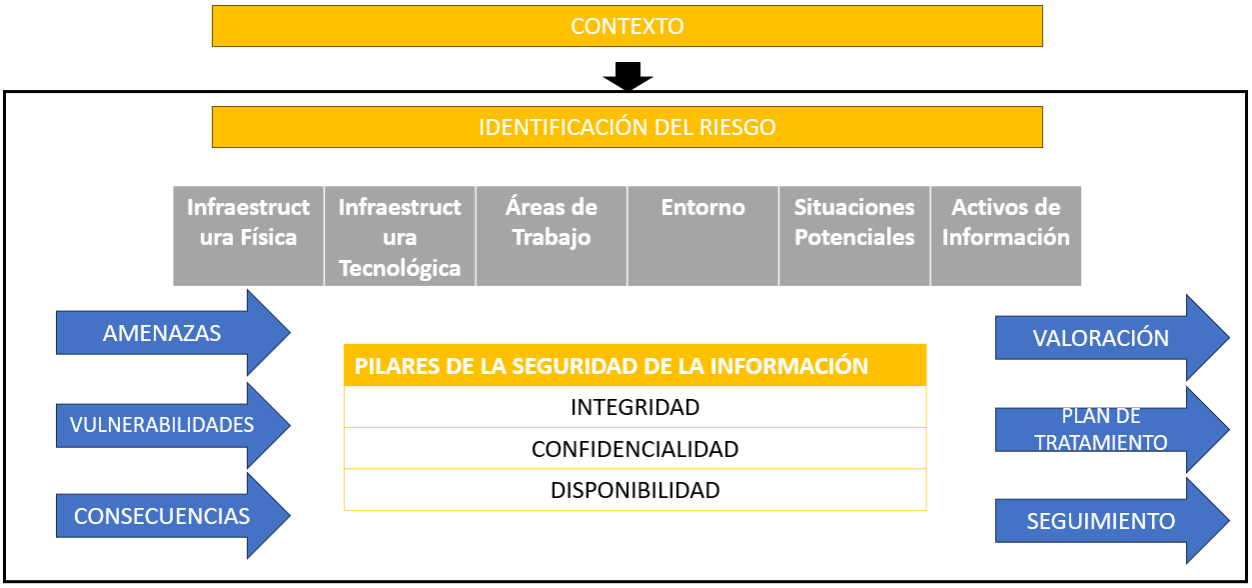
La gestión de riesgos de Seguridad y privacidad de la Información y seguridad digital le permite al COPNIA realizar una identificación, análisis y tratamiento de los riesgos que puedan generar afectación al cumplimiento de los objetivos de sus procesos, contribuyendo en la toma de decisiones, y en la prevención de la materialización de estos. La administración de riesgos de Seguridad y Privacidad de la Información y Seguridad Digital se encuentra enfocada en identificar, analizar, valorar y tratar las amenazas y vulnerabilidades de los activos de información de la entidad, teniendo presente su criticidad y protección. Las etapas presentes en la gestión de riesgos permiten alinearlas con los objetivos, estrategias y políticas corporativas, logrando un nivel de riesgo que pueda aceptar o asumir la Alta Dirección.

8. METODOLOGÍA

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos identificados en la entidad, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016) y alineadas al procedimiento DE-pr-02 Administración del riesgo.

Gestión	Actividades	Tareas	Responsable de la Tarea
Gestión de Riesgos de seguridad y privacidad de la	Actualización de lineamientos de riesgos	Apoyar, cuando se requiera, la actualización de la política, metodología y lineamientos de la gestión de riesgos.	Oficina de Seguridad y Privacidad de la Información

información y seguridad digital	Sensibilización	Socialización de lineamientos y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información y Seguridad Digital	Oficina de Seguridad y Privacidad de la Información
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Contexto, Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información y Seguridad Digital	Oficina de Seguridad y Privacidad de la Información
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Oficina de Seguridad y Privacidad de la Información
	Aceptación de riesgos identificados	Aceptación, aprobación de riesgos identificados y planes de tratamiento	Oficina de Seguridad y Privacidad de la Información y Área de Tecnologías de la Información y las Comunicaciones
	Publicación	Publicación mapa de riesgos del proceso de seguridad y privacidad de la información y de riesgos digitales	Oficina de Seguridad y Privacidad de la Información
	Seguimiento Fase de Tratamiento	Seguimiento a implementación de controles y planes de tratamiento de riesgos los identificados (verificación de evidencias)	Oficina de Seguridad y Privacidad de la Información
	Mejoramiento	Identificación de oportunidades de mejora acorde al seguimiento de la ejecución de los controles y de los planes de tratamiento	Oficina de Seguridad y Privacidad de la Información
		Revisión y/o actualización de lineamientos de Riesgos de Seguridad y privacidad de la información de acuerdo con las observaciones presentadas.	Oficina de Seguridad y Privacidad de la Información
	Monitoreo y revisión	Medición, presentación y reporte de indicadores	Oficina de Seguridad y Privacidad de la Información



Los controles seleccionados serán confrontados con los estándares ISO 27001:2013 y su anexo A; a fin de determinar las falencias del COPNIA en este sentido.

8.1 DESARROLLO METODOLÓGICO

• Fase 1: Análisis de la información

En esta etapa se evaluarán los resultados de las entrevistas con los colaboradores del proceso de tecnologías de la información y de las comunicaciones - TIC, y se desarrollarán las siguientes actividades:

- Aplicar la política de administración del riesgo del COPNIA para tomarla como base del análisis ya que esta tiene definido su propia metodología de gestión de riesgos. En esta metodología se incluyen, entre otros, lo términos y definiciones, los niveles de aceptación del riesgo, los niveles para calificar el impacto, el tratamiento y las periodicidades para el seguimiento, así como las responsabilidades para la ejecución de las actividades.
- Determinar los controles (se desprenden de las medidas) aplicados en el COPNIA.
- Determinar los riesgos que van a ser incluidos en el Plan de Tratamiento de Riesgos.

• Fase 2: Desarrollo de los proyectos

En esta fase se realizarán las actividades que permitan la estructuración de las medidas.

- Determinar el nombre de la medida.
- Definir los responsables de cada medida.
- Establecer el objetivo de cada medida.
- Elaborar la justificación de la medida.
- Definir las actividades a realizar para el desarrollo de la medida.

• **Fase 3: Análisis de los proyectos**

- Definición de los controles relacionados con cada medida.
- Validar los riesgos mitigados por cada medida.
- Análisis de la aplicabilidad de las medidas.
- Priorización de las medidas.

• **Fase 4: Definición del organigrama de responsabilidad**

En esta fase se realizará un organigrama y se definirán responsabilidades respecto a la administración y gestión del riesgo, esta etapa deberá ser definida por el COPNIA teniendo en cuenta su estructura organizacional para la gestión de riesgos.

- Identificación de las funciones del COPNIA en materia de seguridad de la información.
- Definición del grupo de trabajo de gestión de riesgo por parte del COPNIA.
- Definición de las funciones del grupo de trabajo referentes a la aplicación y gestión de las medidas.

• **Fase 5: Ciclo de vida del tratamiento de riesgos**

Definir las actividades a realizar por cada uno de los elementos del ciclo de vida del Plan de Tratamiento de Riesgos.

Planear: Dentro de esta etapa se desarrollan las actividades definidas en la fase 1 de la metodología de tratamiento de riesgos.

Hacer: En este paso del ciclo de vida se desarrollarán las actividades enmarcadas en la fase 2 de la metodología del tratamiento de riesgos.

Verificar: En esta etapa se desarrollarán las actividades que permiten hacer seguimiento o auditorías a la ejecución de cada una de las medidas.

Actuar: Dentro de esta etapa se realizarán las mejoras teniendo en cuenta el seguimiento y los resultados de las auditorías de la ejecución de los proyectos.

Establecimiento del contexto

El contexto en términos generales relaciona los aspectos externos, internos y del proceso que se deben tener en cuenta para gestionar los riesgos de Seguridad y Privacidad de la Información y Seguridad Digital del COPNIA, contenidos en **el mapa de riesgos de seguridad digital**. A partir del contexto es posible establecer las posibles causas de los riesgos a identificar. De esta forma, para la definición del contexto, se seguirán las metodologías dispuestas en la entidad para lograr establecer las posibles causas y determinar la identificación de los riesgos.

Identificación del riesgo

Para la identificación de riesgos de Seguridad y Privacidad de la Información y Seguridad Digital del COPNIA se debe tener en cuenta diferentes aspectos como infraestructura física, áreas de trabajo, entorno y ambiente en general, para lo cual se hace indispensable que cada uno de los procesos tenga identificado los activos de información (de acuerdo con las definiciones dadas por el Programa de Gestión Documental de la Entidad), y reconocer las situaciones potenciales que causarían daño a la entidad poniendo en riesgo el logro de los objetivos establecidos.

La falta de apropiación en temas referentes a la seguridad de la información o la ausencia de controles (vulnerabilidades) puede ser aprovechadas por una amenaza causando la materialización de un riesgo (Incidente), por lo que es preciso identificar: El atributo de la triada de la información afectado (Confidencialidad, Integridad, Disponibilidad), el proceso dueño del riesgo, activo de información afectado, amenazas, vulnerabilidades y consecuencias.

Para la identificación se pueden abarcar datos históricos, análisis teóricos, opiniones informadas y expertas, y las necesidades de las partes involucradas.

Valoración del riesgo

La valoración de los riesgos de Seguridad y Privacidad de la Información y Seguridad Digital del COPNIA, contenidos en **el mapa de riesgos de seguridad digital,** se realizará acorde a la metodología para la administración de riesgos mencionada en la Guía para la administración del riesgo y el diseño de controles en entidades públicas emitida por el Departamento Administrativo de la Función Pública y MINTIC.

Es así como en el análisis adelantado por la Oficina de Seguridad y Privacidad de la Información a los procesos se analiza el contexto, se identifican los riesgos y se realiza el análisis de la probabilidad e impacto como valoración preliminar para identificar el nivel del riesgo inherente, asociando sus vulnerabilidades e identificando los controles para mitigarlas. A estos controles se le identifican las variables a evaluar para el adecuado diseño de controles como son: responsable, periodicidad, propósito, cómo se realiza la actividad de control, observaciones o desviaciones y la evidencia de la ejecución del control. Adicionalmente se evalúa que cada control se ejecute de manera consistente, de tal forma que pueda mitigar el riesgo. Esta valoración se realiza de acuerdo con las tablas y metodología establecida y mencionada en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP.

Para los riesgos de interrupción, se indica que los controles identificados pueden ser transversales, partiendo del criterio denominado custodio del activo, puesto que cuando dicho custodio es un proceso diferente al proceso que identifica el riesgo o es un tercero, estos controles y planes de tratamiento deben establecerse de manera conjunta. El proceso donde se identifica el riesgo aporta los niveles de probabilidad, impacto y riesgo inherente que genera la posible indisponibilidad del activo

Definición y aprobación de mapas de riesgos y planes de tratamiento.

Una vez concluidas las etapas de la administración de riesgos y se obtenga la valoración de los riesgos de Seguridad y Privacidad de la Información y Seguridad Digital del COPNIA, contenidos en **el mapa de riesgos de seguridad digital**, el Sub Comité de seguridad y privacidad de la información debe revisar y recomendar el mapa de riesgos, para que este sea adoptado por la entidad. De igual forma en este documento aprobarán los planes de tratamiento con las actividades requeridas que permitan mitigar aquellos riesgos cuyo nivel residual este en zona Moderada, Alta o Extrema.

Materialización

En el caso de materializarse un riesgo, este debe ser reportado de acuerdo con el procedimiento de gestión de incidentes TIC-pr-01, por la categoría de seguridad de la información. Así mismo, se deberá analizar el riesgo y validar en qué nivel queda posterior a la materialización, registrando los cambios respectivos en el mapa de riesgos. En caso de que se materialice un riesgo que no esté identificado, deberá ser reportado para que se inicie su correspondiente identificación en **el mapa de riesgos de seguridad digital**.

Oportunidad de Mejora

El COPNIA no sólo deberá centrarse en los riesgos identificados, sino que este análisis o apreciación del riesgo debe ser la base para identificar oportunidades. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo

9. RECURSOS

El COPNIA, en el marco de la gestión de riesgos de Seguridad y Privacidad de la información, y Seguridad Digital, dispone de los siguientes recursos.

9.1 RECURSOS VARIABLE

Humanos:

• El profesional de gestión de Seguridad y Privacidad de la Información y el sub comité de seguridad y privacidad de la información.
• Líderes y gestores de procesos
• Área de TIC del COPNIA
• Grupo de Trabajo de COLCERT
• Grupo de Trabajo de CSIRT

Técnicos

- Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital del DAFP
- Matriz de riesgos del proceso de seguridad y privacidad de la información COPNIA, cuya gestión del riesgo se maneja dentro del Sistema de Gestión de Calidad de la entidad.
- Mapa de riesgos de seguridad digital, cuya gestión del riesgo se maneja dentro del plan de tratamiento de riesgos de seguridad y privacidad de la información.

Logísticos

Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos en el PIC (Plan Institucional de Capacitación) que se encuentre vigente para la Entidad.

Financieros

Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías en Seguridad y Privacidad de la Información - que se manejará acorde al Plan anual de adquisiciones vigente para la entidad.

10. PRESUPUESTO PARA LA IMPLEMENTACIÓN DE CONTROLES

La estimación y asignación del presupuesto para el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y Seguridad Digital identificados en la entidad corresponderá al dueño del riesgo (líder del proceso), quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos y del plan de tratamiento de riesgos de seguridad y privacidad de la información. Estos serán incluidos dentro del plan de adquisiciones vigente para la entidad.

11. MEDICIÓN

El monitoreo y seguimiento de los riesgos de Seguridad y Privacidad de la Información y Seguridad Digital del COPNIA , así como de sus controles y planes de tratamiento, contenidos en **el mapa de riesgos de seguridad digital,** se realiza por parte de la Oficina de Seguridad y Privacidad de la Información, teniendo en cuenta la periodicidad y fechas de cumplimiento establecidas, validando los resultados de los seguimientos realizados así como el cargue de los soportes correspondientes a los controles definidos.

Una vez los procesos realicen el reporte de cumplimiento de sus planes de tratamiento y controles, la oficina de Seguridad y Privacidad de la Información realiza la revisión y validación de esta información, con el fin de reportar la medición de la gestión del riesgo a través del indicador que tiene como propósito medir el nivel de implementación de los controles de los riesgos de Seguridad y Privacidad de la Información y Seguridad Digital del COPNIA.

La medición se realiza con un indicador que está orientado principalmente a determinar el porcentaje de ejecución de los controles definidos para mitigar los riesgos identificados en los sistemas de gestión de la entidad.

Nombre del indicador: Nivel de implementación de los controles de riesgos digitales.
Tipo de indicador: Eficacia.
Responsable: Oficina de seguridad y privacidad de la información.
Fuente: Seguimiento de la matriz de riesgos digitales y materialización en los tickets de servicio.
Objetivo: Medir el nivel de implementación de los controles para los riesgos de seguridad digital.
Frecuencia de análisis: Trimestral.
Formula: Porcentaje de controles implementados SGC y SGSI / # total de controles definidos

Metas:

85%-100% - ALTO
60%-84% - MEDIO
0%- 59% - BAJO

12. ANEXOS

No aplica

13. CONTROL DE CAMBIOS

No.	Fecha	Descripción del cambio o modificación
1	Enero 2024	Primera emisión. Aprobado en Comité Institucional de Gestión y Desempeño (Acta 05-2024)

ALVARO IVAN TORRES GONZALEZ Firmado digitalmente por ALVARO IVAN TORRES GONZALEZ Fecha: 2024.01.31 08:04:16 -05'00'	Firmado digitalmente por MARICELA OYOLA MARTINEZ	RUBEN DARIO OCHOA ARBELAEZ Firmado digitalmente por RUBEN DARIO OCHOA ARBELAEZ
ALVARO IVÁN TORRES GONZÁLEZ	**MARICELA OYOLA MARTÍNEZ**	**RUBÉN DARÍO OCHOA ARBELÁEZ**
Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información	Subdirector Administrativo y Financiero	Director General
ACTUALIZÓ	**REVISÓ**	**APROBÓ**