



REPÚBLICA DE COLOMBIA
COPNIA
Consejo Profesional Nacional de Ingeniería

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

2024 - 2026

TABLA DE CONTENIDO

1. INTRODUCCIÓN.....	3
2. MARCO NORMATIVO	3
3. MISIÓN Y VISIÓN DE LA ENTIDAD	4
4. DEFINICIONES	5
5. OBJETIVOS	6
6. ALCANCE	6
7. MARCO REFERENCIAL	7
7.1. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS	7
8. METODOLOGÍA.....	8
8.1 DESARROLLO METODOLÓGICO.....	9
A. Análisis de la información	9
B. Identificación del riesgo	9
C. Valoración del riesgo	9
D. Control del riesgo.....	10
E. Monitoreo de riesgos.....	11
F. Materialización	11
G. Oportunidad de Mejora	14
9. RECURSOS	14
9.1 RECURSOS VARIABLE.....	14
10. PRESUPUESTO PARA LA IMPLEMENTACIÓN DE CONTROLES	15
11. DESARROLLO DEL PLAN	15
12. MEDICIÓN	16
13. ANEXOS	17
14. CONTROL DE CAMBIOS	17

1. INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y Seguridad Digital del COPNIA, definidos en **el mapa de riesgos de seguridad digital de la Entidad**, tiene como objetivo identificar, evaluar y mitigar los riesgos asociados con la gestión de la información dentro de la organización. Este plan es una respuesta estructurada a las amenazas y vulnerabilidades, con el fin de garantizar que los controles de seguridad sean adecuados y eficaces para minimizar los impactos negativos en caso de incidentes de seguridad. La seguridad de la información no solo es esencial para proteger la integridad, confidencialidad disponibilidad y autenticidad de los datos, sino también para mantener la confianza de los usuarios, cumplir con las normativas legales y garantizar la continuidad de las operaciones.

Este plan está alineado con los principios del **ciclo de vida de la seguridad de la información**, basado en la mejora continua, y se complementa con las políticas internas de seguridad, la legislación aplicable y las mejores prácticas internacionales, como las directrices de la ISO/IEC 27001.

La implementación eficaz de este plan de tratamiento de riesgos contribuye al fortalecimiento de la postura de seguridad de la Entidad y permite la toma de decisiones informadas para proteger los activos más críticos frente a riesgos emergentes.

Así mismo, el presente plan establece el marco de acción para el tratamiento de los riesgos de seguridad de la información, asegurando la protección de los activos críticos y la alineación con los objetivos estratégicos de la Entidad. Su implementación y mejora continua permitirá fortalecer la resiliencia y el cumplimiento normativo en el COPNIA.

2. MARCO NORMATIVO

El marco normativo se toma como referente acorde a la naturaleza jurídica del Consejo Profesional Nacional de Ingeniería COPNIA y, en este sentido, lo que sea aplicable a la Entidad, la cual se encuentra publicada así:

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

Así mismo, se toma como referencia la normativa general así:

- **Constitución Política de Colombia** (Artículo 15): Reconoce el derecho fundamental a la intimidad y a la protección de los datos personales, estableciendo la obligación del Estado de garantizar su respeto
- **Ley 1581 de 2012**: Régimen General de Protección de Datos Personales, que regula el tratamiento de datos y la implementación de políticas para su protección en entidades públicas y privadas.

- **Ley 1712 de 2014:** Ley de Transparencia y del Derecho de Acceso a la Información Pública, que regula el acceso y protección de la información pública.
- **Documento CONPES 3995 de 2020:** Política Nacional de Confianza y Seguridad Digital, que promueve la protección de datos e infraestructura crítica, fortaleciendo la gestión de riesgos en el entorno digital.
- **Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital del Departamento Administrativo de la Función Pública (DAFP):** Define lineamientos para gestionar riesgos de seguridad digital en entidades públicas
- **Guía de gestión de riesgos de seguridad y privacidad de la información (MINTIC):** busca orientar a las Entidades a gestionar los riesgos de Seguridad de la información basado en los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad) buscando la integración con la Metodología de riesgos del DAFP.

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 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 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

- Identificar, evaluar y gestionar los riesgos de seguridad y privacidad de la información de manera estructurada los cuales están contenidos en el **mapa de riesgos de seguridad digital**, de acuerdo con el contexto establecido para la Entidad.
- Garantizar la protección de la confidencialidad, integridad y disponibilidad de la información.
- Garantizar el cumplimiento de requisitos legales, reglamentarios, regulatorios y de las normas técnicas colombianas, aplicables a la seguridad y privacidad de la información.
- Fomentar una cultura organizacional de seguridad y conciencia mediante el fortalecimiento y apropiación del conocimiento interno referente a la gestión de riesgos de Seguridad y Privacidad de la información y seguridad digital, del COPNIA.
- Asegurar la mejora continua en la gestión de riesgos de seguridad y privacidad de la información.

6. ALCANCE

Implementar 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 todos los procesos de la entidad que gestionen, procesen o almacenen información de valor, y de esta manera establecer buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos institucionales. Adicionalmente, este plan brinda 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

El marco referencial del plan de gestión de riesgos de seguridad de la información se basa en estándares, normativas y metodologías reconocidas a nivel internacional y local, asegurando un enfoque estructurado y alineado con las mejores prácticas, como base fundamental la Entidad cuenta con una Política de Administración del riesgo en la cual 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 cumplimiento 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 segunda línea de defensa, es decir, los subdirectores, jefes de dependencias y líderes o responsables 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. En este caso se deben tomar medidas de contingencia, es decir, que se deben definir acciones bajo el supuesto de que el riesgo se materialice.

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.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se fundamentará en un marco de referencia, que incorpore las normativas nacionales, estándares internacionales y lineamientos de transformación digital, el Modelo de Seguridad y Privacidad de la Información (MSPI) y los nuevos estándares internacionales como ISO/IEC 27001:2022.

Este marco permitirá alinear sus controles de seguridad con las mejores prácticas y garantizar la protección de los datos sensibles de las poblaciones vulnerables. La implementación de tecnologías emergentes como inteligencia artificial (IA) y Blockchain se realizará bajo principios éticos y responsables. Estas tecnologías serán evaluadas en términos de impacto en la privacidad y seguridad de la información. La protección de datos sensibles se priorizará a través de la adopción de herramientas tecnológicas y estrategias para gestionar de forma segura los datos, en cumplimiento con las nuevas exigencias regulatorias.

8. METODOLOGÍA

A continuación, se describe el ciclo de actividades que se ejecutarán para la gestión de riesgos de seguridad y privacidad de la información, tomando como base 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.

8.1 DESARROLLO METODOLÓGICO

A. Análisis de la información

En esta etapa se evaluarán los resultados de las entrevistas con los colaboradores de los diferentes procesos de la Entidad, 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, los 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.
- Revisar 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.
- Identificación de activos: Los líderes de proceso serán responsable de priorizar los activos calificados con un nivel de riesgo alto, así como aquellos adicionales que considere relevantes para la generación de los riesgos

B. 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 identificados 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.

C. 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

D. Control del riesgo

De acuerdo con los riesgos identificados, se establecerán los controles necesarios para mitigar o tratar cada uno de ellos, alineados con el Modelo de Seguridad y Privacidad de la Información (MSPI). Para ello, la Entidad se basará en los controles propuestos por la NTC-ISO/IEC 27001 con el fin de reducir la probabilidad de materialización de los riesgos y minimizar el impacto de los incidentes de seguridad

Los controles seleccionados serán confrontados con los estándares ISO 27001y su anexo A, los cuales contemplan los siguientes criterios:

- A.5 Políticas de seguridad de la información
- A.6 Organización de la seguridad de la información
- A.7 Seguridad ligada a los recursos humanos
- A.8.1 Responsabilidad por los activos
- A.9 Control de acceso
- A.10 Criptografía
- A.11 Seguridad física y del ambiente
- A.12 Seguridad de las operaciones
- A.13 Seguridad de las comunicaciones
- A.14 Adquisición, desarrollo y mantenimiento del sistema
- A.15 Relaciones con el proveedor
- A.16 Gestión de incidentes de seguridad de la información
- A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio
- A.18 Cumplimiento

Así mismo, para mitigar los riesgos identificados, se implementarán, entre otros los siguientes controles basados en estándares internacionales:

- **Controles técnicos:**
 - Implementación de firewalls y sistemas de detección de intrusos.

- Cifrado de datos en tránsito y en reposo.
- Control de accesos mediante autenticación multifactorial.
- Monitoreo continuo de redes y sistemas.
- Gestión de parches y actualizaciones de software.
- **Controles administrativos:**
 - Políticas y procedimientos de seguridad de la información.
 - Gestión de identidades y accesos.
 - Evaluaciones de riesgos y auditorías internas periódicas.
 - Planes de continuidad del negocio y recuperación ante desastres.
 - Sensibilización y capacitación en seguridad para los funcionarios.
- **Controles físicos:**
 - Seguridad en el acceso a instalaciones y servidores.
 - Uso de sistemas de control de acceso biométrico.
- **Controles de cumplimiento:**
 - Alineación con normativas como ISO/IEC 27001, y lineamientos de normativas nacionales
 - Contratos y acuerdos de confidencialidad con terceros.
 - Revisión y actualización de políticas de seguridad de la información

E. Monitoreo de riesgos

Se debe realizar seguimientos trimestrales del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, durante los cuales se analizan y verifican los avances de las actividades establecidas. Estos seguimientos incluyen la emisión y publicación de informes detallados, los cuales permiten evaluar el cumplimiento de las acciones previstas y garantizar la efectividad de las medidas implementadas en la mitigación de los riesgos identificados en **el mapa de riesgos de seguridad digital**.

Este proceso debe seguir aplicándose de manera continua para asegurar la mejora constante y el cumplimiento de los objetivos del plan

F. 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**.

Una vez identificado el incidente este deberá ser reportado conforme a la siguiente matriz de escalamiento del incidente:

No.	Actividad	Responsable	Descripción
1	Informar el incidente de seguridad de la información	Funcionario que identifica el incidente	El funcionario que identifica el incidente debe reportar a través de la herramienta de servicio de tickets, reportar el incidente conforme al procedimiento TIC-pr-01, por la categoría de seguridad de la información
2	Coordinar acciones correctivas	Profesional de Gestión área TIC/Profesional de gestión de la Oficina de Seguridad y Privacidad de la información	Coordinar con los responsables de soporte técnico, que éstos hayan ejecutado o ejecuten con prontitud, todas las acciones que se requieran para asegurar y fortalecer los componentes de tecnologías de la información (si aplica)
3	Reportar afectación en infraestructura tecnológica (Si aplica)	Profesional de Gestión área TIC/Profesional de gestión de la Oficina de Seguridad y Privacidad de la información	Cuando algún componente de la infraestructura tecnológica (sitios Web, aplicaciones, servicios en línea, sistemas de información, entre otros) de la Entidad, haya sido vulnerado o comprometido, se reportará en primera instancia al ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia) por medio de correo electrónico a: contacto@colcert.gov.co o al Teléfono: (+571) 2959897. Así mismo se debe reportar ante el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Digital). para el respectivo apoyo y coordinación en la gestión de estos a través del

No.	Actividad	Responsable	Descripción
			<p>formato de reporte establecido por el CSIRT Gobierno, el cual estará disponible por los canales de comunicación autorizados:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Csirtgob@mintic.gov.co <input type="checkbox"/> 01 8000 910742 Opción 3.
4.	Reportar incidente informático	Profesional de Gestión área TIC/Profesional de gestión de la Oficina de Seguridad y Privacidad de la información/Representante Jurídico de la Entidad	<p>Informar al CAI Virtual de la Policía Nacional www.ccp.gov.co, Centro Cibernético Policial de la Policía Nacional al teléfono 4266900 ext. 104092, para recibir asesoría del caso en particular y posterior judicialización. Establecer los procedimientos internos que adopta el Consejo Profesional Nacional de Ingeniería – COPNIA para la implementación de la Política de Protección y Tratamiento de Datos Personales en concordancia con las disposiciones legales vigentes.</p>
5.	Reportar incidente de seguridad que afecte las bases de datos registradas	Profesional de gestión de la Oficina de Seguridad y Privacidad de la información	<p>Si el incidente compromete la privacidad de los datos de las bases de datos registradas ante la Superintendencia de Industria y Comercio, se deberá reportar a la SIC para esto se deberá hacer el reporte de los incidentes de seguridad dentro de los quince (15) días hábiles siguientes al momento en que se detecten mediante el aplicativo dispuesto para tal fin en la página web de</p>

No.	Actividad	Responsable	Descripción
			la Superintendencia de Industria y Comercio en el micrositio de la Delegatura para la Protección de Datos Personales o mediante cualquiera de los canales habilitados por la entidad para recibir comunicaciones, es decir, al correo electrónico contactenos@sic.gov.co y/o físicamente en la Carrera 13 No. 27-00 piso 1.

G. 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 VARIABLES

Humanos:

- El profesional de gestión de Seguridad y Privacidad de la Información y el subcomité de seguridad de la información.
- Líderes 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. DESARROLLO DEL PLAN

En el marco del Plan de Tratamiento de Riesgos de Seguridad y privacidad de la Información, se desarrollará un conjunto de actividades estratégicas orientadas a fortalecer la gestión integral de riesgos y garantizar la protección de los activos de información institucionales. Estas acciones se realizarán de manera cíclica anual (2024 - 2026) incluyen la revisión y actualización de documentos, la sensibilización y capacitación del personal, la identificación y evaluación de riesgos, la implementación de controles, y el monitoreo y mejora continua del plan, conforme a esto a continuación se presentan las actividades a realizar:

Actividad	Responsable	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Revisión y actualización del plan de tratamiento de riesgos de seguridad y privacidad de la información	Profesional de gestión Oficina de seguridad y privacidad de la información												
Revisión , identificacion y actualización de riesgos digitales	Profesional de gestión Oficina de seguridad y privacidad de la información/Profesionales de gestión todos los proceso												
Revisión y actualización de controles y sus planes de tratamiento	Profesional de gestión Oficina de seguridad y privacidad de la información												
Definición/actualización de inventario de activos	Profesional de gestión Oficina de seguridad y privacidad de la información/Profesional de gestión Área TIC/Profesional de Gestión Área Administrativa/Lideres de Proceso												
Definición/actualización de procedimientos requeridos	Profesional de gestión Oficina de seguridad y privacidad de la información/Lideres de Proceso												
Implementación/seguimiento de procedimientos	Profesional de gestión Oficina de seguridad y privacidad de la información/Profesional de gestión Área TIC/Profesional de Gestión Área Administrativa												
Seguimiento controles y tratamiento	Profesional de gestión Oficina de seguridad y privacidad de la información												
Socialización de lineamientos para el tratamiento de riesgos de seguridad y privacidad de la Información	Profesional de gestión Oficina de seguridad y privacidad de la información												
Identificar oportunidades de mejora basado en los resultados de la evaluación del riesgo	Profesional de gestión Oficina de seguridad y privacidad de la información												

12. 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

13.ANEXOS

No aplica

14.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)
2	Marzo 2025	Actualización de introducción, objetivos, metodología y desarrollo del plan.

JOHANNA CAÑÓN LONDOÑO	ÁNGELA PATRICIA ÁLVAREZ LEDESMA	MARICELA OYOLA MARTÍNEZ	RUBÉN DARÍO OCHOA ARBELÁEZ
Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información (E)	Subdirectora de Planeación, Control y Seguimiento	Subdirectora Administrativa y Financiera	Director General
ACTUALIZÓ	REVISÓ	REVISÓ	APROBÓ