REPÚBLICA DE COLOMBIA
CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA COPNIA

RESOLUCIÓN NACIONAL
R2025031943
22 julio de 2025

Por medio de la cual se actualiza y modifica la Política de Seguridad y privacidad de la información para el Consejo Profesional Nacional de Ingeniería – COPNIA

El director general del Consejo Profesional Nacional de Ingeniera – COPNIA en ejercicio de las facultades que le otorga el artículo séptimo y el artículo octavo numeral 8 de la Resolución Nacional R2024040897 del 23 de septiembre de 2024, el Manual Específico de Funciones y Competencias Laborales Vigente, y;

CONSIDERANDO

Que el Consejo Profesional Nacional de Ingeniería – COPNIA, es una entidad *sui géneris* especial e independiente de derecho público del orden nacional, creada por la Ley 94 de 1937, y actualmente regulada por los artículos 25, 26, 27 y siguientes de la Ley 435 de 1998 y las leyes 842 de 2003, 1325 de 2009 y 1796 de 2016; encargada de la función administrativa de inspección y vigilancia del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares (artículo 26 de la Constitución Política), motivo por el cual, a través de las actuaciones administrativas correspondientes, expide las matrículas profesionales, los certificados de inscripción profesional y los certificados de matrícula –actos administrativos – que constituyen la autorización del Estado para ejercer dichas profesiones, y adelanta en ejercicio de la acción disciplinaria ético profesional, como Tribunal de Ética, las investigaciones disciplinarias ético profesionales, a través del procedimiento administrativo de carácter sancionatorio establecido en la Ley 842 de 2003, modificada por la Ley 1796 de 2016, a los profesionales bajo su control que vulneren el Código de Ética Profesional establecido en la misma normatividad.

Que la Ley 1341 de 2009, definió los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones.

Que el artículo 17 de la Ley Estatutaria 1581 de 2012, "Régimen General de Protección de Datos Personales", y el artículo 2.2.2.25.3.1. del Decreto 1074 de 2015, "Decreto Único Reglamentario del Sector Comercio Industria y Turismo", consagraron la necesidad de garantizar de forma integral la protección y el ejercicio del derecho fundamental de Habeas Data y estableció dentro de los deberes de los responsables del tratamiento de datos personales, desarrollar políticas para este derecho.

Que el Decreto 2573 de 2014, establece los lineamientos generales de la Estrategia de Gobierno en Línea y en Desarrollo de este define los instrumentos para su implementación.

Que el Decreto 108 de 2015, subrogado por el artículo 1 del Decreto 767 de 2022 determinó que uno de los habilitadores de la Política de Gobierno Digital es el de Seguridad y Privacidad de la Información, el cual busca que los sujetos obligados desarrollen capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en

Documento Firmado digitalmente lo cual garantiza su plena validez jurídica y probatoria (Ley 527 de 1999).

todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos

Que el Decreto 1083 de 2015 en su artículo 2.2.22.2.1 establece las políticas de Gestión y Desempeño Institucional, incluidas las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".

Que el Manual para la implementación de Gobierno Digital, versión 6 de diciembre de 2018, establece la Seguridad de la Información como un elemento transversal habilitador de la política de Gobierno Digital

Que la Resolución 500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones, establece lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establece los lineamientos y estándares para la estrategia de seguridad digital, a los sujetos obligados señalados en el artículo 2.2.9.1.1.2. del Decreto 1078 de 2015, así mismo el artículo 5 de la misma Resolución, establece que los sujetos obligados deben adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital. Dicha estrategia se debe incluir en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos artículo 2.2.22.3.14. del capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, o la norma que la modifique, adicione, subrogue o derogue. Así como, adoptar el Modelo de Seguridad y Privacidad de la Información – MSPI señalado en el Anexo 1 de la misma resolución, como habilitador de la política de Gobierno Digital.

Que el documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, para orientar y dar los lineamientos respectivos a las entidades.

Que el Departamento Administrativo de la Función Pública conceptuó con radicado 20166000253021 del 06 de diciembre de 2016 " ...esta Dirección considera que, si bien el Consejo Nacional Profesional de Ingeniería COPNIA es de naturaleza publica, no hace parte de alguna de las Ramas del Poder Público ni del nivel central y descentralizado de la administración pública, en consecuencia, no estará obligado a implementar el Modelo Estándar de Control Interno MECI definido en la Ley 87 de 1993"

Además, que el Departamento Administrativo de la Función Pública conceptuó con radicado 20195000058751 del 27 de febrero de 2019 que "*si bien por las características de su entidad no hacen parte de alguna de las Ramas del Poder Público ni del nivel central y descentralizado, son una entidad de naturaleza pública, por lo que atendiendo el mandato constitucional citado deberán garantizar la aplicación de adecuados mecanismos y métodos de control interno, para que las actuaciones que se surtan en virtud de la administración de su entidad estén dirigidas al adecuado cumplimiento de los fines del Estado*." además "…*las políticas de gestión y desempeño contenidas en el Modelo Integrado de Planeación y Gestión MIPG, deben ser aplicadas acorde con las normas que las regulan, por lo que si bien su entidad no está obligada a implementar integralmente el modelo deberán analizar dichas políticas e implementarlas en la medida en que les sean aplicables de acuerdo con las normas que las regulan, evitando posibles incumplimientos y para la mejora en la prestación de servicios a sus usuarios*".

Como parte de las modificaciones realizadas a la estructura orgánica del COPNIA, mediante la Resolución Nacional R2023015884 del 27 de abril de 2023, "Por la cual se modifica la

estructura orgánica del Consejo Profesional Nacional de Ingeniería - COPNIA y se actualizan las funciones de unas dependencias y áreas", se creó la Oficina de Seguridad y Privacidad de la Información, la cual tiene entre sus funciones el liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la entidad; gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información; y, definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implementación de las medidas de seguridad en la Entidad, entre otras.

Que mediante la Resolución Nacional R2024043248 del 2 de octubre de 2024 se actualizó el Modelo Integrado de Planeación y Gestión del COPNIA, como un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de la entidad, conforme a las particularidades propias de la naturaleza jurídica de la entidad. Una de las políticas de gestión y desempeño que desarrolla el Modelo Integrado de Planeación y Gestión es "Gobierno Digital

Que conforme con lo expuesto; mediante Resolución Nacional 1332 de 2014 se adoptó el Sistema de Seguridad de la Información, la política de seguridad, los objetivos y el alcance de este en el Copnia, y se hace necesario realizar una revisión de la política de seguridad y privacidad de la información actual frente a la nueva normatividad y el direccionamiento estratégico de la Entidad.

Que por lo anteriormente expuesto;

RESUELVE

ARTÍCULO PRIMERO. COMPROMISO CON LA SEGURIDAD DE LA INFORMACIÓN. El Consejo Profesional Nacional de Ingeniería – COPNIA adopta la Política de Seguridad y Privacidad de la Información de la siguiente manera:

"*En el ejercicio del cumplimiento de su misión institucional, el Consejo Profesional Nacional de Ingeniería – COPNIA reconoce la importancia de una adecuada gestión de la información comprometido con la implementación de un Sistema de Seguridad de la Información (SGSI) que le permita proteger la integridad, disponibilidad y confidencialidad de los activos de información y establecer un marco de confianza en el ejercicio de su misión con el Estado y los ciudadanos enmarcado en el cumplimiento normativo,.*"

ARTÍCULO SEGUNDO. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La Política de Seguridad y Privacidad de la Información tiene como objetivo proporcionar orientación institucional y establecer los lineamientos que garanticen que el acceso a la información se realice únicamente por personas con una necesidad legítima de conocerla, en función de sus responsabilidades (confidencialidad); que dicha información esté protegida contra modificaciones no autorizadas, ya sean intencionales o accidentales (integridad); que esté disponible cuando se requiera (disponibilidad); y que sea utilizada exclusivamente para los fines para los cuales fue recolectada (privacidad).

Esta política se fundamenta en el Modelo de Seguridad y Privacidad de la Información, las directrices de Seguridad Digital y Gobierno Digital, los requisitos legales aplicables y las necesidades de las partes interesadas.

En este marco, el **Consejo Profesional Nacional de Ingeniería (COPNIA)**, en cumplimiento de su compromiso con la seguridad y privacidad de la información, establece los siguientes objetivos:

1. Fortalecer la cultura de seguridad de la información en los funcionarios, terceros y usuarios del COPNIA.
2. Establecer las políticas y procedimientos en materia de seguridad y privacidad de la información.
3. Fortalecer la mejora continua del Sistema de Gestión de Seguridad de la Información.
4. Definir los controles necesarios para la protección de los activos de la entidad y la reducción de riesgos.
5. Cumplir con los requisitos legales, reglamentarios y regulatorios en materia de seguridad y privacidad de la información, seguridad digital y protección de la información personal.

ARTÍCULO TERCERO. ALCANCE DE LA POLÍTICA. La Política de Seguridad y Privacidad de la Información proporciona el marco para la implementación de un modelo de seguridad confiable, orientado al desarrollo de directrices propias de su gestión.

La Política de Seguridad y Privacidad de la Información constituye un componente fundamental dentro del desarrollo de la Política de Gobierno Digital, en el marco de las políticas de gestión y desempeño establecidas por el Modelo Integrado de Planeación y Gestión del COPNIA.

Esta política aplica a todos los procesos establecidos en la Entidad y debe ser atendida por los funcionarios, contratistas y terceros que tengan injerencia en la gestión de la entidad, en todas sus sedes.

ARTICULO CUARTO. METODOLOGÍA PARA LA IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. La metodología para la implementación de la Política de Seguridad y Privacidad de la Información se encuentra definida en el respectivo manual de seguridad de la información, y se gestiona y controla conforme al Procedimiento de Control de Documentos definido por el COPNIA.

ARTÍCULO QUINTO. NIVELES DE RESPONSABILIDAD. Los niveles de responsabilidad respecto a la Política de Seguridad y Privacidad de la Información serán los siguientes:

Responsable	**Responsabilidad**
Dirección General	Proporcionar los recursos necesarios para la implementación y mantenimiento del sistema de gestión de seguridad de la información (Recursos económicos, formación y recursos tecnológicos).
Comité Institucional de Gestión y Desempeño	Articular los esfuerzos institucionales, recursos, metodologías y estrategias para asegurar la implementación, sostenibilidad y mejora del Modelo Integrado de Planeación y Gestión del COPNIA. Asegurar la implementación de las Políticas de Gestión y Desempeño Institucional. Aprobar los planes que se formulen para la implementación de las Políticas de Gestión y Desempeño, en concordancia con el Modelo Integrado de Planeación y Gestión del COPNIA.

Responsable	**Responsabilidad**
Subcomité de Seguridad de la Información	Presentar recomendaciones para la implementación de políticas, planes, programas y proyectos en materia de seguridad de la información y controles en la implementación de sistemas o servicios. Impulsar la implementación del Sistema de Gestión de Seguridad de la Información - SGSI. Servir de facilitador y punto de apoyo para el desarrollo de iniciativas de proyectos de seguridad. Recomendar roles y responsabilidades que se relacionen con la seguridad de la información. Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad. Acompañar e impulsar el desarrollo de proyectos de seguridad y privacidad de la información. Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad. Proponer y/o recomendar al Comité Institucional de Gestión y Desempeño, metodologías, acciones, documentos, diagnósticos, planes, políticas y procesos específicos para la seguridad de la información.
Área de Tecnologías de la Información y las Comunicaciones	Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información.
Oficina de Seguridad y Privacidad de la Información	Analizar, definir, documentar y gestionar el plan de seguridad y privacidad de la información y proponer las decisiones que permitan gestionar la seguridad de la información en el marco del cumplimiento de la política y los lineamientos definidas y aprobados por la entidad. Apoyar en la generación de los lineamientos (Manuales, procedimientos y formatos) que permitan el establecimiento y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información en la Entidad.
Área de Gestión Humana	Asegurar que los funcionarios tomen conciencia de sus responsabilidades en seguridad de la información y las cumplan a través del Plan Institucional de Capacitaciones. Garantizar la aplicación de la seguridad y privacidad de la información de acuerdo con las políticas y procedimientos establecidos.
Área de Contratación	Verificar y garantizar la implementación de las medidas de seguridad de la información en la gestión con los contratistas de la entidad. Garantizar la protección de la seguridad y privacidad de la información de todos los activos de la información que puedan verse involucrados, mediante el seguimiento e implementación de cláusulas en los contratos.
Área de Relacionamiento Interinstitucional y Comunicaciones	Apoyar las actividades de comunicación y sensibilización en seguridad de la información, para difundir la información en todos los niveles de la entidad.

Responsable	Responsabilidad
Oficina de Control Interno	Incluir la seguridad de la información dentro de los planes de auditoría institucionales. Apoyar en situaciones de posibles violaciones a las políticas de seguridad de la información.
Oficina de Control Interno Disciplinario	Adelantar las investigaciones disciplinarias en casos de posibles violaciones a las políticas de seguridad y privacidad de la información por parte de los funcionarios de la Entidad.
Lideres de proceso	Implementar la política y procedimientos de seguridad de la información que se definan como parte del SGSI.
Todos los funcionarios y contratistas	Cumplir a cabalidad la política y procedimientos de seguridad de la información definidos y aprobados

ARTÍCULO SEXTO. SANCIONES. Cualquier violación a las políticas de seguridad y privacidad de la información deberá ser sancionada de acuerdo con el Código General Disciplinario y las leyes y estatutos de la ley colombiana.

ARTÍCULO SÉPTIMO. REVISIÓN La Política de Seguridad y Privacidad de la Información, será revisada anualmente o antes, si se dieran cambios estructurales en la entidad que afecten el cumplimiento de la política o en caso de incidentes de seguridad de la información que requieran cambios en la política.

ARTÍCULO SEXTO VIGENCIA Y DEROGACIONES. La presente Resolución rige a partir de la fecha de su expedición y deroga la Resolución Nacional 1027 de 2019. y las demás disposiciones que le sean contrarias.

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., a los veintidos (22) días del mes de julio (7) del año dos mil veinticinco (2025).

RUBEN DARÍO OCHOA ARBELÁEZ
Director General

Revisó: Ángela Patricia Álvarez Ledesma – Subdirectora de Planeación, Control y Seguimiento
Revisó: Álvaro Iván Torres González – Profesional de gestión del Área de Tecnologías de la Información y las Comunicaciones
Elaboró: Johanna Cañon Londoño – Profesional de gestión de la Oficina de Seguridad y Privacidad de la Información

Copia en papel auténtica de documento electrónico. La validez de este documento puede verificarse ingresando a: https://atencionalciudadano.copnia.gov.co/Pages/Index.aspx Agregue los siguientes datos R2025031943 y 040e

Documento Firmado digitalmente lo cual garantiza su plena validez jurídica y probatoria (Ley 527 de 1999).