REPÚBLICA DE COLOMBIA
CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA COPNIA

RESOLUCIÓN NACIONAL
R2025030612
14 julio de 2025

Por medio de la cual se actualiza la Política de Gestión y Desempeño de Seguridad Digital 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.

Conforme lo indica el ámbito de aplicación del Decreto 1078 de 2015 respecto a la estrategia de Gobierno Digital – GD -, las entidades públicas deben realizar la implementación del Modelo de Seguridad y Privacidad de la información - MSPI – con el objetivo de conformar un Sistema de Gestión de Seguridad de la Información al interior de la entidad. El MSPI integra en cada una de sus fases tareas asociadas a la gestión de riesgos de seguridad digital, ya que esta práctica constituye su base fundamental.

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 lo expuesto, a partir de la Resolución Nacional 2068 del 24 de diciembre de 2019, se adoptó la Política de Gestión y Desempeño de Seguridad Digital y se hace necesario revisar la política frente a las actualizaciones del Manual Operativo de MIPG, considerando la naturaleza jurídica de la Entidad para actualizar lo que sea necesario.

En mérito de lo expuesto,

RESUELVE

TITULO I

COMPROMISO, OBJETIVO Y ALCANCE DE LA POLÍTICA DE SEGURIDAD DIGITAL

ARTÍCULO 1. Compromiso con la Seguridad Digital. El Consejo Profesional Nacional de Ingeniería- COPNIA mantiene su compromiso con el diseño y fortalecimiento de medidas para identificar, gestionar, tratar, controlar y mitigar los riesgos inherentes de seguridad digital en los que se puedan comprometer los activos de información, mediante la implementación de

medidas que garanticen la confidencialidad, disponibilidad e integridad de la información que gestiona la Entidad.

ARTÍCULO 2. Objetivo de la Política de Seguridad Digital. El propósito es establecer una metodología que permita proteger los sistemas de información y recursos digitales contra cualquier amenaza informática que afecte la seguridad cibernética o riesgo que pueda comprometer la operatividad y reputación institucional.

ARTÍCULO 3. Alcance de la Política. La Política de Seguridad Digital abarca la planificación de la gestión de riesgos de seguridad digital, la implementación de los planes de tratamiento de los riesgos definidos, el monitoreo y revisión, y el mejoramiento continuo de la gestión del riesgo de seguridad digital.

Así mismo, aplica a todos los funcionarios de la Entidad, sistemas y activos de información, así como proveedores y terceros que manejen información de la Entidad

TÍTULO II

METODOLOGÍA GENERAL PARA LA IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL

ARTICULO 4. Generalidades. La metodología para la implementación y seguimiento de la Política de Seguridad Digital es definida por la Dirección General a través de la Oficina de Seguridad y Privacidad de la Información, con el acompañamiento del Área de Tecnologías de la Información y las Comunicaciones, conforme a la normatividad aplicable al Consejo Profesional Nacional de Ingeniería, de acuerdo con su naturaleza jurídica.

El Subcomité de Seguridad de la Información revisa y presenta recomendaciones para la implementación de la Política de Seguridad Digital al Comité Institucional de Gestión y Desempeño.

Para facilitar la implementación de la política, el COPNIA podrá utilizar como referencia herramientas orientadoras emitidas por otras entidades públicas.

CAPÍTULO I

GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

ARTICULO 5. Planificación de Riesgos de Seguridad Digital. La planificación de la gestión de riesgos de Seguridad Digital se realiza de manera armonizada con los lineamientos de seguridad y privacidad de la información que se encuentran en la política de Gestión y Desempeño de Gobierno Digital, y obedeciendo a la metodología definida por la Entidad para la administración de riesgos. La Planificación comprende:

- Definición del contexto interno, externo y de los procesos de la Entidad.
- Definición de la política de administración del riesgo.
- Designación de roles y responsabilidades.
- Definición de criterios de probabilidad, impacto y zonas de riesgo aceptable.
- Identificación de activos de información.
- Identificación de riesgos.

- Valoración de riesgos.
- Definición del tratamiento de los riesgos.

ARTICULO 6. Implementación y seguimiento. Corresponde al Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información liderar, coordinar, supervisar y acompañar el proceso de implementación de los planes de tratamiento de riesgos de seguridad digital, verificando que los responsables de los planes ejecuten las tareas en los tiempos pactados y que los recursos se estén ejecutando de acuerdo con lo planeado.

ARTÍCULO 7. Monitoreo y revisión. De acuerdo con las responsabilidades establecidas en los diferentes procedimientos de la Entidad se realizan las siguientes actividades de monitoreo y revisión.

- Registro y reporte de incidentes de seguridad digital.
- Reporte de la gestión del riesgo de seguridad digital al interior de la Entidad.
- Reporte de la gestión del riesgo de seguridad digital a autoridades o entidades especiales.
- Auditorías internas y externas.
- Medición del desempeño.

ARTÍCULO 8. Mejoramiento continuo de la gestión de seguridad digital. El líder de la Oficina de Seguridad y Privacidad de la Información debe coordinar, con quien corresponda, la definición de las acciones para mejorar continuamente la gestión de riesgos de seguridad digital de la siguiente forma:

- Revisar y evaluar los hallazgos encontrados en las auditorías internas, otras auditorías e informes de los entes de control realizadas.
- Establecer las posibles causas y consecuencias del hallazgo.
- Determinar si existen otros hallazgos similares para establecer acciones correctivas y evitar así que se lleguen a materializar.
- Emprender acciones de revisión continua, que permitan gestionar el riesgo a tiempo, disminuir el impacto y la probabilidad de ocurrencia del riesgo detectado, así como la aparición de nuevos riesgos que puedan afectar el desempeño de la Entidad o de los servicios que presta al ciudadano.

ARTÍCULO 9. Comunicación y capacitación. El COPNIA adelanta acciones de sensibilización, concientización y capacitación que permita que los funcionarios comprendan y apropien la metodología para la implementación y seguimiento de la Política de Seguridad Digital en cada una de sus etapas.

Corresponde al Profesional de Gestión de la Oficina de Seguridad y Privacidad de la Información el desarrollar planes de formación y sensibilización incorporando el componente de seguridad digital en diferentes niveles. Las acciones se realizan en coordinación con el responsable del Área de Gestión Humana a través del Plan Institucional de Capacitación, y del Área de Relacionamiento Interinstitucional y Comunicaciones con el Plan de trabajo de comunicación interna que establezca la Entidad.

ARTÍCULO 10. Vigencia. La presente Resolución rige a partir de la fecha de su expedición y deroga la Resolución 2068 de 2019 y las demás disposiciones que le sean contrarias.

REPÚBLICA DE COLOMBIA
COPNIA
Consejo Profesional Nacional de Ingeniería

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., a los catorce (14) días del mes de julio (7) del año dos mil veinticinco (2025).

RUBÉN DARIO OCHOA ARBELAEZ
Director general

Revisa: Ángela Patricia Álvarez Ledesma - Subdirectora de planeación, control y seguimiento
Revisa: Álvaro Iván Torres González – Profesional de gestión del Área de Tecnologías de la Información y las Comunicaciones
Revisa: Johanna Cañon Londoño – Profesional de gestión de la Oficina de Seguridad y Privacidad de la información
Proyecta: Rafael Andrés Forero Contreras – Profesional de gestión de la Subdirección de Planeación, Control y Seguimiento

---

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 R2025030612 y ba7c