REPÚBLICA DE COLOMBIA

COPNIA

Consejo Profesional Nacional de Ingeniería

RESOLUCIÓN 2068

24 DIC 2019

"Por medio de la cual se adopta la Política de Gestión y Desempeño de Seguridad Digital para el Copnia"

El Director General del Consejo Profesional Nacional de Ingeniería – COPNIA en ejercicio de las facultades que le otorga los numerales 23 y 30, del artículo cuarto de la Resolución Nacional 362 del 30 de marzo de 2016 modificada por la Resolución 795 de 2017, y

CONSIDERANDO:

Que el Consejo Profesional Nacional de Ingeniería – COPNIA, es una entidad sui géneris o 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, Certificados de Inscripción Profesional y 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 Profesional, las investigaciones disciplinarias ético profesionales, a través del procedimiento administrativo de carácter sancionatorio establecido en las leyes 842 de 2003 y 1796 de 2016, a los profesionales bajo su control que vulneren el Código de Ética Profesional establecido en la misma.

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 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."

Que mediante la Resolución Nacional 498 de abril de 2019 se adoptó 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 "Seguridad Digital"

RESUELVE:

TITULO I

COMPROMISO, OBJETIVO Y ALCANCE DE LA POLÍTICA DE SEGURIDAD DIGITAL

ARTÍCULO 1. Compromiso con la seguridad digital: El Consejo Profesional de Ingeniería- COPNIA mantiene su compromiso de gestionar los riesgos inherentes de seguridad digital que acarrea el entorno digital de la Entidad.

ARTÍCULO 2. Objetivo de la Política de Seguridad Digital: El propósito de esta política es contrarrestar el incremento de las amenazas informáticas que afecten significativamente y afrontar retos en aspectos de seguridad cibernética.

ARTÍCULO 3. Alcance 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.

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 del área de Tecnología de la Información y de las Comunicaciones, conforme a la normatividad aplicable al Consejo Profesional Nacional de Ingeniería de acuerdo a su naturaleza jurídica.

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

ARTÍCULO 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 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 de 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.

ARTÍCULO 6. Ejecución. Corresponde al líder del área de Tecnología de la Información y de las Comunicaciones supervisar y acompañar el proceso de implementación de los planes de tratamiento de riesgos, 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 a las responsabilidades establecidas en los procedimientos de administración de riesgos y de auditorías, 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 del riesgo de seguridad digital. El líder del área de Tecnología de la Información y de las Comunicaciones 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 pública o de los servicios que presta al ciudadano.

ARTÍCULO 9. Vigencia. La presente Resolución rige a partir de la fecha de su expedición y deroga las disposiciones que le sean contrarias.

COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá D.C., a los veinticuatro (24) días del mes de diciembre del año dos mil diecinueve (2019).

RUBÉN DARÍO OCHOA ARBELÁEZ
Director General

Proyecta: ANGELA PATRICIA ALVAREZ LEDESMA – Profesional de gestión de la Subdirección de Planeación, Control y Seguimiento
Revisa: ALVARO IVÁN TORRES – Profesional de gestión del área de Tecnología de la Información y de las Comunicaciones